PENINGKATAN KEAMANAN SMART DOOR LOCK BERBASIS IOT MENGGUNAKAN PENGENALAN WAJAH BERBASIS ARTIFICIAL INTELLIGENCE DENGAN METODE LIVENESS DETECTION

Sub Judul:

RANCANG BANGUN SISTEM PENGENALAN WAJAH DENGAN MOBILEFACENET DAN METODE *LIVENESS DETECTION* SEBAGAI MEKANISME ANTI-SPOOFING PADA RASPBERRY PI

SKRIPSI

FAHRUL ROSI

2207421052

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

RANCANG BANGUN SISTEM PENGENALAN WAJAH DENGAN MOBILEFACENET DAN METODE *LIVENESS DETECTION* SEBAGAI MEKANISME ANTI-SPOOFING PADA RASPBERRY PI

SKRIPSI

Dibuat Untuk Melengkapi Syarat Syarat yang Diperlukan Untuk
Memperoleh Diploma Empat Politeknik

FAHRUL ROSI

2207421052

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2026

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini :

Nama	:	Fahrul Rosi
Nim	:	2207421052
Jurusan	:	Teknik Informatika dan Komputer
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Rancang Bangun Sistem Pengenalan Wajah Dengan MobileFaceNet dan Metode *Liveness Detection* Sebagai Mekanisme *Anti-Spoofing* Pada Raspberry Pi

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjukan sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila dikemudian hari terbukti atau dapat dibuktikan dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

POLITEKNIK NEGERI JAKARTA

Depok, 29 Juni 2026

Yang membuat pernyataan,

(Fahrul Rosi)

Nim. 2207421052

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAAN

Skripsi diajukan oleh:

Nama	:	Fahrul Rosi
Nim	:	2207421052
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Rancang Bangun Sistem Pengenalan Wajah Dengan MobileFaceNet dan Metode *Liveness Detection* Sebagai Mekanisme *Anti-Spoofing* Pada Raspberry Pi

Telah diuji oleh tim dalam Sidang Skripsi pada hari Kamis, Tanggal 2, Bulan Juli Tahun 2026, dan dinyatakan LULUS.

Disahkan Oleh:

Pembimbing I	Asep Kurniawan, S.Pd., M.Kom.	( )
Penguji I	Dr. Indra Hermawan, S.Kom., M.Kom.	( )
Penguji II	Ariawan Andi Suhandana, S.Kom., M.T.I.	( )
Penguji III	Dwi Ermawati, MT	( )

Mengetahui :

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.

NIP. 197908032003122003

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, nikmat, pertolongan, dan kemudahan-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Rancang Bangun Sistem Pengenalan Wajah Dengan MobileFaceNet dan Metode Liveness Detection Sebagai Mekanisme Anti-Spoofing Pada Raspberry PI". Selama proses penyusunan skripsi ini, penulis mendapatkan banyak dukungan, dan segala bantuan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT atas segala kekuatan, petunjuk, dan kemudahan yang diberikan kepada penulis.
2. Kedua orang tua dan keluarga yang selalu memberikan doa, kasih sayang, dukungan, serta menjadi alasan penulis untuk terus berusaha menyelesaikan pendidikan ini.
3. Bapak Asep Kurniawan, S.Pd., M.Kom. selaku dosen pembimbing yang dengan sabar telah memberikan arahan, bimbingan, masukan, serta kepercayaan dan ruang bagi penulis untuk belajar dan berproses dari awal hingga akhir penyusunan skripsi ini.
4. Kurniawan Sandi selaku rekan kelompok penulis yang bersedia bekerja samadalam menyelesaikan skripsi ini.
5. Orang-orang berharga yang telah memberikan nasihat, semangat, dan keyakinan kepada penulis untuk tetap menyelesaikan proses ini.
6. Seluruh dosen, civitas akademika Politeknik Negeri Jakarta, khususnya Program Studi Teknik Multimedia dan Jaringan, serta teman-teman seperjuangan yang telah memberikan ilmu, pengalaman, bantuan, dan dukungan selama masa perkuliahan hingga penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diterima. Semoga skripsi ini dapat memberikan manfaat dan menjadi kontribusi dalam pengembangan teknologi Internet of Things, khususnya pada bidang sistem mekanisme kontrol akses *smart door lock*.

Depok, 29 Juni 2026

Fahrul Rosi

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini :

Nama	:	Fahrul Rosi
Nim	:	2207421052
Jurusan	:	Teknik Informatika dan Komputer
Program Studi	:	Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Rancang Bangun Sistem Pengenalan Wajah Dengan MobileFaceNet dan Metode *Liveness Detection* Sebagai Mekanisme *Anti-Spoofing* Pada Raspberry PI

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsisaya tanpa meminta izin darisaya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, 29 Juni 2026

Yang Menyatakan,

(Fahrul Rosi)

NIM. 2207421052

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Rancang Bangun Sistem Pengenalan Wajah Dengan MobileFaceNet dan Metode Liveness Detection Sebagai Mekanisme Anti-Spoofing Pada Raspberry PI

ABSTRAK

Sistem pengenalan wajah pada smart door lock konvensional sangat rentan terhadap spoofing attack 2D menggunakan foto atau video, serta mengalami degradasi akurasi pada pencahayaan tidak ideal. Penelitian ini bertujuan merancang dan mengimplementasikan smart door lock menggunakan Raspberry Pi 4 Model B yang aman dari pemalsuan dan andal di berbagai kondisi cahaya. Metode yang digunakan menggunakan pendekatan kuantitatif dengan riset eksperimental untuk mengombinasikan framework MediaPipe Face Mesh (ekstraksi 468 facial landmarks 3D), model AI MobileFaceNet (Cosine Similarity), algoritma CLAHE untuk perbaikan kontras, serta mekanisme liveness detection (head pose dan blink detection) sebagai penyaring keaktifan subjek. Hasil eksperimen menunjukkan fungsionalitas sistem berjalan 100% dan sukses menolak seluruh serangan pemalsuan foto cetak maupun video secara mutlak (100%). Pada jarak optimal 40 cm, sistem mempertahankan rata-rata Cosine Score sebesar 96,76% (normal), 73,91% (low-light), dan 71,04% (backlight). Pengujian klasifikasi biometrik menghasilkan akurasi global 97,04%, presisi 98,72%, sensitivitas 97,89%, dan F1-Score 98,31%, dengan suhu CPU harian yang dingin di angka 48,3°C. Dapat disimpulkan bahwa sistem pengenalan wajah dengan liveness detection yang dibangun terbukti mampu mengatasi pemalsuan wajah berupa foto dan video dalam mengamankan hak akses pintu.

Kata Kunci: ***Smart Door Lock*, *Liveness Detection*, *Anti-Spoofing*, *MobileFaceNet, MediaPipe Face Mesh, Raspberry Pi.***

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME ii
LEMBAR PENGESAHAAN iii
KATA PENGANTAR iv
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS v
ABSTRAK vi
DAFTAR ISI vii
DAFTAR GAMBAR x
DAFTAR TABEL xi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 4
1.4 Tujuan dan Manfaat Penelitian 5
1.4.1 Tujuan Penelitian 5
1.4.2 Manfaat Penelitian 5
1.5 Sistematika Penulisan 6
BAB II TINJAUAN PUSTAKA 8
2.1 Penelitian Sejenis 8
2.2 Smart Door Lock 9
2.3 Raspberry Pi 10
2.4 MediaPipe Face Mesh 10
2.5 Liveness Detection 11
2.5.1 Head Pose Estimation 11
2.5.2. Blink Detection 11
2.6 MobileFaceNet 12
2.7 Evaluasi Performa Klasifikasi Biometrik 12
BAB III METODE PENELITIAN 14
3.1 Rancangan Penelitian 14
3.2 Tahapan Penelitian 15
3.3 Objek Penelitian 16
BAB IV HASIL DAN PEMBAHASAN 18
4.1 Analisis Kebutuhan 18
4.1.1 Analisis Kebutuhan Perangkat Keras (*Hardware*) 18
4.1.2 Analisis Kebutuhan Perangkat Lunak 22
4.1.3 Analisis Kebutuhan Fungsional dan Non-Fungsional 23
4.2 Perancangan Sistem 25
4.2.1 Blok Diagram 26
4.2.2 Arsitektur Sistem 27
4.2.3 Diagram Alir 28
4.2.4 Rancangan Skematik Alat 30
4.2.5 Rancangan Basis Data 34
4.3 Implementasi Sistem 40
4.3.1 Implementasi Perangkat Keras 40
4.3.2 Implementasi Perangkat lunak 41

4.3.3 Implementasi Basis Data 54
4.4 Pengujian 59
4.4.1 Deskripsi Pengujian 59
4.4.2 Prosedur Pengujian 60
4.4.3 Data Hasil Pengujian 60
BAB V PENUTUP 85
5.1 Kesimpulan 85
5.2 Saran 85
DAFTAR PUSTAKA 87
DAFTAR RIWAYAT HIDUP 91
LAMPIRAN 92

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR GAMBAR

Gambar 3. 1 Tahapan Penelitian 15
Gambar 4. 1 Blok Diagram 26
Gambar 4. 2 Arsitektur Sistem 27
Gambar 4. 3 Diagram Alir Proses Pendaftaran 28
Gambar 4. 4 Diagram Alir Proses Verifikasi 29
Gambar 4. 5 Rancangan Skematik Alat 30
Gambar 4. 6 Rancangan Basis Data SQLite 35
Gambar 4. 7 Rancangan Basis Data Supabase 37
Gambar 4. 8 Implementasi Perangkat Keras 40
Gambar 4. 9 Tampilan Halaman Utama 42
Gambar 4. 10 Deteksi Wajah Menggunakan Facemesh 43
Gambar 4. 11 Pose Liveness 44
Gambar 4. 12 Liveness Kedipan Mata (Bling Eye) 45
Gambar 4. 13Ekstraksi Fitur Biometrik 45
Gambar 4. 14Pencocokan Wajah Kondisi Normal 46
Gambar 4. 15Pencocokan Wajah Kondisi Cahaya Backlight 47
Gambar 4. 16Pencocokan Wajah pada Kondisi Cahaya Low Light 48
Gambar 4. 17 Liveness Pose Kepala Acak 49
Gambar 4. 18 Liveness Kedipan Mata (Blink Eye) 49
Gambar 4. 19 Deteksi Serangan Layar Video 50
Gambar 4. 20 Deteksi Serangan Foto Cetak 51
Gambar 4. 21Tampilan Akses Berhasil 52
Gambar 4. 22 Tampilan Akses Ditolak 53
Gambar 4. 23Basis Data Lokal Wajah Pengguna 55
Gambar 4. 24 Basis Data Supabase Wajah Pengguna 55
Gambar 4. 25Basis Data Lokal Log Registrasi 56
Gambar 4. 26 Basis Data Supabase Log Registrasi 56
Gambar 4. 27 Basis Data Lokal Akses Pintu 57
Gambar 4. 28 Basis Data Supabase Akses Pintu 57
Gambar 4. 29 Basis Data Lokal Log Serangan 58
Gambar 4. 30Basis Data Supabase Log Serangan 58

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 2.1 Penelitian Sejenis 8
Tabel 4.1 Hardware Unit Pemroses Citra 18
Tabel 4.2 Hardware Unit Kontrol dan Aktuator Fisik 20
Tabel 4.3 Kebutuhan Perangkat Lunak 22
Tabel 4.4 Kebutuhan Fungsional 24
Tabel 4.5 Kebutuhan Non-Fungsional 25
Tabel 4.6 Subsistem Manajemen Daya 31
Tabel 4.7 Subsistem Pengolahan Citra Visual 32
Tabel 4.8 Subsistem Antarmuka Visual 32
Tabel 4.9 Subsistem Aktuator dan Saklar Logika 33
Tabel 4.10 Subsistem Input Manual 34
Tabel 4.11 Deskripsi Fungsi Tabel Basis Data 38
Tabel 4.12 Pengujian Fungsional 61
Tabel 4.13 Performa Pada Mode *Register* 65
Tabel 4.14 Performa Pada Mode Verifikasi 67
Tabel 4.15 Analisis Waktu Latensi Tahap Registrasi (*Preprocessing*) 69
Tabel 4.16 Skenario Spoofing Menggunakan Foto 70
Tabel 4.17 Skenario Spoofing Menggunakan Video 72
Tabel 4.18 Pengujian Jarak Deteksi 40 cm 76
Tabel 4.19 Pengujian Jarak Deteksi 60 cm 77
Tabel 4.20 Pengujian Jarak Deteksi 80 cm 79
Tabel 4.21 Pengujian Jarak Deteksi 100 cm 81
Tabel 4.22 Skenario penggunaan Topi 84
Tabel 4.23 Skenario Pengggunaan Kacamata 86
Tabel 4.24 Skenario Penggunaan Masker 88
Tabel 4.25 Skenario Kondisi *Lowlight* 91
Tabel 4.26 Skenario Kondisi *Backlight* 93
Table 4.27 Hasil Pengujian 96
Tabel 4.28 Perhitungan Metrik 96

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi *Internet of Things* (IoT) telah mengalami akselerasi yang sangat pesat baik pada skala global maupun nasional. Secara global, IoT telah mentransformasi berbagai sektor industri melalui interkoneksi miliaran perangkat pintar yang saling bertukar data secara otonom melalui jaringan internet (Harbi et al., 2021). Di Indonesia, tren adopsi teknologi IoT mendorong digitalisasi pada berbagai aspek kehidupan, termasuk sektor domestik. Salah satu manifestasi paling signifikan dari perkembangan ini adalah munculnya konsep *smart home*, di mana infrastruktur rumah diintegrasikan dengan jaringan nirkabel untuk meningkatkan efisiensi dan kenyamanan penghuni (Chakraborty et al., 2023). Di dalam ekosistem *smart home*, tren penerapan IoT kini sangat berfokus pada *smart security system* (sistem keamanan pintar), mengingat aspek perlindungan aset dan pencegahan kerentanan keamanan fisik merupakan prioritas utama dalam manajemen hunian modern (Chakraborty et al., 2023).

Dalam sistem keamanan modern, IoT memegang peran yang sangat krusial sebagai fondasi arsitektur pemantauan dan pengendalian jarak jauh. Paradigma keamanan konvensional yang bersifat pasif kini bergeser menuju sistem kontrol akses yang aktif, adaptif, fleksibel, dan bekerja secara *real-time* (Chakraborty et al., 2023). Kebutuhan akan sistem kontrol akses yang handal didorong oleh meningkatnya kompleksitas ancaman keamanan fisik dan mobilitas manusia yang tinggi. Fleksibilitas komunikasi pada ekosistem ini memungkinkan pengelolaan hak akses serta pemantauan kondisi hunian dilakukan secara dinamis melalui perangkat seluler pintar dari mana saja dan kapan saja (Ahwadti & Setiawan, 2025).

Sistem penguncian pintu pintar atau *smart door lock* berbasis IoT merupakan salah satu komponen utama dalam implementasi *smart security system* yang menawarkan efisiensi tinggi dibandingkan dengan mekanisme kunci mekanis konvensional (Harke et al., 2022). Kunci konvensional memiliki keterbatasan inheren, seperti risiko kehilangan kunci fisik serta ketiadaan sistem pencatatan riwayat akses. Sebaliknya, *smart door lock* berbasis IoT menawarkan pemantauan digital,

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

eliminasi ketergantungan pada replika kunci fisik, serta kemampuan integrasi dengan sistem kendali pusat rumah pintar (Ahwadti & Setiawan, 2025). Dengan memanfaatkan komputer papan tunggal (*single-board computer*) sebagai unit pemroses utama, *smart door lock* mampu mengeksekusi perintah penguncian dan pembukaan pintu secara otomatis dengan efisiensi tinggi pada arsitektur *edge environment* (Harbi et al., 2021).

Sejumlah penelitian terdahulu telah berupaya melakukan eksperimen dan implementasi sistem keamanan berbasis pengenalan wajah dan IoT. Penelitian oleh (Ahwadti & Setiawan, 2025) merancang sistem keamanan pintu rumah menggunakan *face recognition* berbasis IoT dengan modul ESP32-CAM yang berhasil mengenali wajah pengguna, namun masih memerlukan optimalisasi pada sisi anti-*spoofing*. Selanjutnya, (Harke et al., 2022) mengimplementasikan sistem *smart door lock* berbasis pengenalan wajah untuk mengatasi masalah keamanan kunci fisik, namun belum menyertakan evaluasi ketahanan terhadap serangan presentasi (*presentation attack*). Eksperimen lain dilakukan oleh Wijaya et al. yang mengimplementasikan *face recognition* berbasis CNN menggunakan *library* dlib dan OpenCV untuk sistem presensi dengan akurasi tinggi. Temuan ini juga sejalan dengan riset (Dewi & Ismawan, 2021) bahwa penerapan algoritma CNN terbukti sangat superior untuk pemrosesan komputer visi *face recognition*.

Meskipun teknologi *face recognition* berbasis *deep learning* seperti *Convolutional Neural Network* (CNN) menawarkan akurasi pengenalan yang tinggi (Dewi & Ismawan, 2021), sistem ini memiliki kelemahan yang sangat fatal terhadap serangan pemalsuan identitas atau *spoofing attack*. Sistem pengenalan wajah standar umumnya hanya menganalisis fitur visual dua dimensi tanpa memverifikasi keaslian dari objek yang dipindai (George et al., 2022). Akibatnya, sistem autentikasi ini sangat rentan dieksploitasi menggunakan *presentation attack*, yang meliputi penggunaan foto cetak resolusi tinggi (*print attack*), rekaman video digital yang diputar ulang melalui layar *smartphone* (*video replay attack*), maupun penggunaan topeng tiga dimensi (George et al., 2022). Kerentanan ini menyebabkan integritas *smart door lock* menjadi lemah, karena penyerang dapat dengan mudah memalsukan hak akses hanya dengan menggunakan representasi visual dari wajah pengguna sah.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Sebagai solusi untuk mengatasi kelemahan kritikal pada sistem biometrik tersebut, metode *liveness detection* (deteksi keaktifan) atau *face anti-spoofing* dikembangkan dan diimplementasikan secara luas pada sistem autentikasi modern untuk memperkuat pertahanan dari berbagai serangan pemalsuan. *Liveness detection* berfungsi sebagai lapisan proteksi tambahan yang bertugas untuk menganalisis dan memverifikasi apakah input biometrik yang ditangkap oleh sensor kamera berasal dari manusia hidup yang hadir secara fisik pada saat itu (*live subject*), atau berasal dari replika benda mati (*spoofing artifact*). Alasan utama metode ini banyak digunakan adalah kemampuannya dalam mengeksploitasi fitur-fitur dinamis seperti gerakan mata (berkedip), perubahan mikrotekstur kulit, fluktuasi refleksi cahaya, ataupun kedalaman tiga dimensi objek. Dengan mengintegrasikan *liveness detection*, sistem keamanan biometrik dapat secara signifikan mencegah masuknya subjek ilegal ke dalam sistem.

Berdasarkan berbagai keterbatasan tersebut, diperlukan pengembangan sistem *smart door lock* yang mampu mengintegrasikan teknologi IoT, *Face Recognition*, dan *Liveness Detection* dalam satu sistem autentikasi yang berjalan secara lokal (*on-device processing*). Penelitian ini mengimplementasikan perangkat keras komputasi Raspberry Pi 4 Model B yang berfungsi menjalankan proses pengenalan wajah dan deteksi keaktifan secara *real-time* tanpa ketergantungan penuh terhadap layanan *cloud*. Pendekatan komputasi lokal (*edge computing*) ini secara efektif mampu meminimalkan latensi, mengurangi beban *bandwidth* jaringan, dan meningkatkan privasi data pengguna. Mekanisme anti-*spoofing* berbasis *liveness detection* dirancang untuk menganalisis fitur spasial-temporal guna memverifikasi keaslian objek sebelum proses pencocokan wajah dilakukan. Selain itu, penelitian ini juga melakukan evaluasi performa sistem secara komprehensif melalui pengukuran *Accuracy*, *Precision*, *Recall*, dan *F1-Score* untuk memperoleh gambaran menyeluruh mengenai kinerja sistem keamanan pintu pintar yang dikembangkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, celah penelitian utama terletak pada tingginya kerentanan sistem autentikasi wajah konvensional terhadap manipulasi *spoofing* serta tuntutan pemrosesan yang efisien pada perangkat

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

komputasi tepi dengan sumber daya terbatas. Untuk memberikan arah penelitian yang terstruktur, maka rumusan masalah dalam penelitian ini ditetapkan sebagai berikut:

a. Bagaimana merancang dan mengimplementasikan sistem *smart door lock* berbasis IoT yang terintegrasi dengan metode *liveness detection* guna mencegah akses tidak sah akibat serangan pemalsuan wajah (*spoofing*) menggunakan foto atau video?
b. Bagaimana tingkat akurasi sistem pengenalan wajah pada perangkat IoT ketika diuji dalam berbagai kondisi pencahayaan, mulai dari intensitas cahaya rendah (*low-light*) hingga kondisi cahaya latar (*backlight*)?

1.3 Batasan Masalah

Agar pengujian sistem lebih terarah, spesifik, dan objektif, diperlukan pembatasan ruang lingkup penelitian. Pembatasan ini bertujuan untuk menyelaraskan kapasitas komputasi perangkat keras yang digunakan dengan parameter lingkungan fisik selama pengujian. Oleh karena itu, batasan masalah dalam penelitian ini dijabarkan sebagai berikut:

a. Perangkat keras utama yang digunakan sebagai unit pemroses sentral (*edge computing device*) adalah *Single Board Computer* (SBC) Raspberry Pi 4 Model B yang memiliki keterbatasan sumber daya komputasi, sehingga diperlukan optimasi model agar sistem mampu beroperasi secara waktu-nyata (*real-time*).
b. Pengujian metode *liveness detection* difokuskan pada manipulasi akses berupa serangan pemalsuan (*spoofing attack*) dua dimensi (2D), yang meliputi penggunaan media foto cetak (*print attack*) serta foto atau rekaman video yang ditampilkan melalui layar *smartphone* (*replay attack*).
c. Ekstraksi fitur geometri wajah untuk kebutuhan deteksi keaktifan memanfaatkan pustaka MediaPipe Face Mesh, di mana algoritma *liveness detection* tersebut hanya bertindak sebagai gerbang penyaring awal (*anti-spoofing gate*) untuk meloloskan objek hidup sebelum dilanjutkan ke tahap pencocokan identitas wajah.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

d. Evaluasi tingkat akurasi pengenalan wajah dibatasi pada tiga variasi kondisi intensitas pencahayaan, yaitu kondisi normal (siang hari atau lampu ruangan), kondisi cahaya rendah (*low-light*) pada malam hari, serta kondisi cahaya latar (*backlight*) dengan posisi sumber cahaya berada di belakang objek wajah.
e. Sistem kontrol akses yang dirancang menerapkan skema *Single-Factor Authentication* berbasis wajah yang terintegrasi langsung dengan mekanisme *liveness detection* sebagai validasi keaktifan objek secara linier.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian rancang bangun sistem keamanan ini adalah sebagai berikut:

a. Mengimplementasikan sistem *smart door lock* berbasis IoT dengan pengenalan wajah yang aman dari pemalsuan wajah (*foto atau video*) menggunakan metode *liveness detection*.
b. Menganalisis keakuratan pengenalan wajah dalam berbagai kondisi pencahayaan pada perangkat IoT untuk memastikan performa sistem tetap andal.

1.4.2 Manfaat Penelitian

Hasil dari perancangan dan implementasi sistem keamanan ini diharapkan dapat memberikan kegunaan secara teoretis maupun praktis, antara lain:

a. Memberikan kontribusi dalam pengembangan sistem keamanan biometrik, khususnya melalui optimasi fitur *liveness detection* pada perangkat dengan keterbatasan sumber daya (*resource-constrained devices*).
b. Mengurangi risiko terjadinya pembobolan pintu akibat pemalsuan identitas menggunakan media foto maupun video sebagai bentuk serangan *anti-spoofing*.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.5 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini terdiri dari 5 bab, yaitu:

1. BAB I PENDAHULUAN

   Bab I memuat latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan yang berkaitan dengan rancang bangun sistem keamanan pintu pintar (*smart door lock*) berbasis *Internet of Things* dengan integrasi model MobileFaceNet dan metode *liveness detection* pada perangkat Raspberry Pi.
2. BAB II TINJAUAN PUSTAKA

   Bab II berisi tinjauan pustaka dan landasan teori yang membahas konsep *smart door lock*, Raspberry Pi, MediaPipe Face Mesh, *liveness detection* (*head pose estimation* dan *blink detection*), arsitektur MobileFaceNet, evaluasi performa biometrik, serta kajian terhadap penelitian-penelitian terdahulu yang relevan.
3. BAB III METODE PENELITIAN

   Bab III menjelaskan metode penelitian yang digunakan, meliputi rancangan penelitian kuantitatif eksperimental, tahapan pelaksanaan penelitian, perancangan alur citra digital (*raw frame* dan *enhanced frame*), serta objek penelitian pada sasis laboratorium komputer.
4. BAB IV HASIL DAN PEMBAHASAN

   Bab IV memaparkan analisis kebutuhan *hardware* dan *software*, perancangan diagram sirkuit serta basis data hibrida (SQLite dan Supabase), implementasi fisik prototipe, hingga pengujian fungsional, stabilitas perangkat, keandalan *anti-spoofing*, pengaruh jarak/cahaya, dan pengukuran akurasi biometrik.
5. BAB V PENUTUP

   Bab terakhir ini berisi kesimpulan yang merangkum temuan utama penelitian mengenai tingkat keberhasilan dan ketangguhan sistem *smart door lock* dalam mengamankan hak akses dari ancaman manipulasi wajah, serta menyampaikan saran-saran untuk pengembangan sistem di masa mendatang.

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Sejenis

Untuk memperjelas posisi penelitian yang dilakukan, disajikan perbandingan beberapa penelitian sejenis yang relevan. Perbandingan ini digunakan untuk menunjukkan perbedaan metode, platform, serta fokus penelitian sebelumnya, sekaligus menegaskan kebaruan (*novelty*) penelitian yang diusulkan.

Tabel 2.1 Penelitian Sejenis

Jurnal	Hasil	Catatan
(Nur et al., 2024)	**Tujuan:** Penerapan *Face Recognition* untuk model *Smart Lock Door* berbasis IoT guna meningkatkan keamanan pintu. **Teknologi:** ESP32-CAM, FTDI, Solenoid Door Lock, Relay, Algoritma Haar Cascade. **Cara Kerja:** Kamera ESP32-CAM menangkap citra wajah tamu. Citra diproses menggunakan algoritma Haar Cascade. Jika wajah cocok dengan *database*, mikrokontroler mengirim sinyal *LOW* ke Relay untuk mengaktifkan Solenoid dan membuka pintu.	Belum ada fitur ***anti-spoofing*** (rawan dibobol foto) dan akurasi menurun drastis pada cahaya minim.
(Luriansyah et al., 2022)	**Tujuan:** Membangun sistem pengenalan wajah pada keamanan pintu otomatis menggunakan *Single Board Computer*. **Teknologi:** Raspberry Pi 3 Model B, Pi Camera, Solenoid Door Lock, Relay 1 Channel, Metode Eigenface. **Cara Kerja:** Raspberry Pi mengambil data citra melalui Pi Camera. Citra diproses dengan metode Eigenface untuk ekstraksi fitur. Jika wajah dikenali sebagai pemilik, Raspberry Pi memerintahkan Relay untuk mengalirkan daya ke Solenoid Door Lock agar pintu terbuka.	Metode *Eigenface* tergolong klasik (jadul), kurang tangguh untuk variasi wajah, dan tanpa fitur ***liveness detection***.
(Dewi et al., 2025)	**Tujuan:** Membuat sistem presensi perkuliahan yang akurat dan aman dari kecurangan titip absen menggunakan wajah palsu. **Teknologi:** Kamera Laptop/Webcam, Python, YOLOv11 (Deteksi Wajah), InsightFace (Ekstraksi Fitur), Liveness Detection (Blink/Kedipan).	Metode aman, namun implementasi masih berbasis PC/Laptop, belum diterapkan pada perangkat *embedded* (IoT) untuk pintu.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Jurnal	Hasil	Catatan
	Cara Kerja: Sistem mendeteksi wajah secara *real-time*. Sebelum mencocokkan identitas, sistem melakukan *Liveness Detection* dengan mendeteksi kedipan mata. Jika terdeteksi "hidup" dan wajah cocok, presensi dicatat. Jika foto diam, akses ditolak.	
(Yanto et al., 2022)	**Tujuan:** Merancang sistem monitoring keamanan pintu rumah dengan notifikasi jarak jauh kepada pemilik. **Teknologi:** ESP32-CAM, Aplikasi Telegram Bot, Solenoid Door Lock, Power Supply. **Cara Kerja:** ESP32-CAM memantau area pintu. Jika wajah dikenali, kunci terbuka. Jika wajah tidak dikenal atau ada akses paksa, sistem mengambil foto dan mengirimkannya ke Telegram pemilik rumah sebagai peringatan keamanan.	Fokus hanya pada monitoring/notifikasi, belum ada verifikasi keaslian wajah sehingga rentan terhadap pemalsuan.
(Rofiq et al., 2024)	**Tujuan:** Implementasi sistem loker pintar (*Smart Locker*) yang menggantikan kunci fisik dengan wajah untuk efisiensi. **Teknologi:** ESP32-CAM, Modul Relay, Solenoid Lock, Wi-Fi. **Cara Kerja:** Pengguna melakukan registrasi wajah. Saat ingin membuka loker, pengguna menghadapkan wajah ke kamera. Jika data cocok dengan penyimpanan, solenoid loker akan terbuka otomatis tanpa perlu kunci fisik.	Fokus pada efisiensi mekanisme loker, belum memprioritaskan keamanan terhadap serangan *spoofing* (foto wajah).

2.2 Smart Door Lock

Smart Door Lock adalah instrumen keamanan modern yang mengintegrasikan mekanisme kunci mekanis konvensional dengan unit pengontrol elektronik dan modul konektivitas nirkabel guna mengotomatisasi akses pintu (Soedjarwanto et al., 2021). Dalam arsitektur *Internet of Things* (IoT), perangkat ini bertindak sebagai *endpoint* strategis yang menjembatani interaksi fisik antarmuka rumah dengan jaringan digital untuk manajemen hak akses nirkabel. Efektivitas operasional sistem ini sangat bergantung pada keandalan metode verifikasi identitasnya, di mana pemanfaatan karakteristik biometrik visual wajah dinilai paling unggul karena bersifat cepat, mudah digunakan, memiliki sifat non-kontak, serta memanfaatkan fitur unik manusia yang sulit direplikasi atau dipalsukan,

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

sehingga mampu mengeliminasi celah keamanan tradisional seperti risiko kehilangan kunci fisik maupun kebocoran kode PIN (Anwar & Sugiantoro, 2026).

2.3 Raspberry Pi

Raspberry Pi merupakan komputer papan tunggal (*Single Board Computer* atau SBC) berukuran ringkas yang mengintegrasikan komponen komputasi utama dalam satu papan sirkuit sehingga cocok digunakan pada berbagai aplikasi sistem tertanam dan Internet of Things (Cox et al., 2022). Perangkat ini menyediakan pin *General Purpose Input/Output* (GPIO) yang memungkinkan integrasi langsung dengan berbagai sensor dan aktuator, termasuk kamera serta *solenoid door lock* (Makama & Gana, 2021). Dalam paradigma *edge computing*, Raspberry Pi dapat berfungsi sebagai unit pemrosesan lokal yang menjalankan model *machine learning* secara *on-device*, sehingga mampu mengurangi ketergantungan terhadap layanan cloud dan mempercepat respons sistem (Daher et al., 2021). Selain itu, pemrosesan data secara lokal juga berkontribusi terhadap peningkatan privasi karena data sensitif pengguna tidak perlu terus-menerus ditransmisikan melalui jaringan eksternal (Liu et al., 2021).

2.4 MediaPipe Face Mesh

MediaPipe Face Mesh merupakan framework *open-source* berbasis *deep learning* yang dirancang untuk melakukan estimasi geometri wajah secara *real-time* pada perangkat dengan sumber daya komputasi terbatas (Kartynnik et al., 2021). Framework ini mengombinasikan model deteksi wajah BlazeFace dengan jaringan regresi *3D face mesh* yang mampu menghasilkan 468 titik *facial landmarks* tiga dimensi dari satu citra wajah (*monocular image*) secara efisien (Bazarevsky et al., 2021). Dalam konteks *liveness detection*, landmark tersebut menyediakan informasi spasial yang dapat digunakan untuk melacak perubahan posisi pada area mata, alis, dan bibir yang berkaitan dengan gerakan biologis alami pengguna. Selain itu, informasi kedalaman yang direpresentasikan melalui koordinat sumbu Z dapat dimanfaatkan untuk membedakan struktur wajah nyata tiga dimensi dari serangan *spoofing* berbasis foto atau video dua dimensi yang tidak memiliki karakteristik kedalaman wajah asli (Yu et al., 2021).

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.5 Liveness Detection

Liveness detection merupakan teknik keamanan biometrik yang digunakan untuk memastikan bahwa sampel wajah yang diterima sistem berasal dari individu hidup yang benar-benar hadir saat proses autentikasi dan bukan dari media pemalsuan seperti foto, video rekaman, atau replika wajah lainnya (Yu et al., 2021). Teknologi ini bekerja dengan menganalisis karakteristik fisiologis dan perilaku alami manusia, seperti kedipan mata, pergerakan wajah, perubahan ekspresi, serta informasi kedalaman wajah yang sulit direplikasi oleh media spoofing (Yu et al., 2021). Penerapan liveness detection berperan penting dalam meningkatkan keamanan sistem pengenalan wajah karena mampu mendeteksi dan mencegah berbagai bentuk presentation attack, termasuk serangan menggunakan foto dan video replay untuk memperoleh akses tidak sah (George & Marcel, 2021).

2.5.1 Head Pose Estimation

Head pose estimation merupakan teknik dalam bidang *computer vision* yang digunakan untuk menentukan orientasi kepala manusia dalam ruang tiga dimensi berdasarkan informasi yang diperoleh dari citra atau video digital (Asperti & Filippini, 2023). Orientasi kepala umumnya direpresentasikan menggunakan tiga sudut rotasi, yaitu *yaw*, *pitch*, dan *roll*, yang menggambarkan arah pergerakan kepala terhadap sumbu koordinat tiga dimensi (Asperti & Filippini, 2023). Dalam sistem autentikasi berbasis wajah, *head pose estimation* dapat dimanfaatkan sebagai mekanisme *challenge-response* untuk memverifikasi kehadiran pengguna melalui analisis perubahan orientasi kepala yang sesuai dengan instruksi sistem sehingga membantu mengurangi risiko serangan *presentation attack* atau *spoofing* (Algabri et al., 2024).

2.5.2. Blink Detection

Blink detection merupakan metode *liveness detection* pasif yang digunakan untuk mendeteksi kedipan mata sebagai indikator bahwa subjek yang berada di depan kamera merupakan manusia hidup yang aktif berinteraksi dengan sistem (Chuah et al., 2023). Metode ini umumnya menggunakan pendekatan *Eye Aspect Ratio* (EAR) yang dihitung berdasarkan jarak geometris antar titik *facial landmark* pada bagian atas dan bawah mata untuk menentukan kondisi mata terbuka atau tertutup (Dewi et al., 2022). Ketika terjadi kedipan, nilai EAR akan menurun secara signifikan

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

dalam waktu singkat sebelum kembali ke kondisi normal sehingga dapat digunakan sebagai fitur temporal untuk deteksi aktivitas biologis (Fernando et al., 2022). Integrasi blink detection dalam sistem liveness detection sangat penting karena mampu meningkatkan keamanan autentikasi wajah dengan membedakan antara wajah manusia hidup dan serangan spoofing berbasis gambar statis seperti foto cetak (Chuah et al., 2023).

2.6 MobileFaceNet

MobileFaceNet merupakan arsitektur *Lightweight Convolutional Neural Network* yang dirancang secara khusus untuk mengeksekusi tugas *face recognition* dan *face verification* pada perangkat dengan keterbatasan sumber daya komputasi seperti Raspberry Pi (Xu et al., 2021). Desain model ini berfokus pada minimalisasi jumlah parameter dan kompleksitas komputasi melalui konfigurasi jaringan CNN yang efisien untuk mengekstraksi representasi karakteristik unik wajah menjadi sebuah *feature vector* (*embeddings*) berdimensi 128 (Liu et al., 2021). Pada penerapannya, efisiensi komputasi tersebut dioptimalkan melalui konversi model ke format ONNX (*Open Neural Network Exchange*) citra input 112×112 piksel RGB yang dieksekusi menggunakan *runtime* khusus untuk mempercepat durasi pemrosesan inferensi secara lokal. Pendekatan arsitektur tepi (*edge computing*) ini berhasil memangkas latensi waktu respon pemindaian wajah secara signifikan dengan konsumsi daya yang rendah, sebelum akhirnya matriks data embeddings tersebut dicocokkan menggunakan kalkulasi matematis *Cosine Similarity* secara *real-time* tanpa mengurangi performa akurasi sistem (Xu et al., 2021).

2.7 Evaluasi Performa Klasifikasi Biometrik

Pengujian ini dilakukan untuk menganalisis performa komputasi model MobileFaceNet dalam mengklasifikasikan objek wajah berdasarkan metrik evaluasi standar machine learning. Parameter yang diuji meliputi Akurasi, Precision, Recall, dan F1-Score untuk mengukur keandalan serta persentase galat prediksi model, di mana representasi matematis dari rumus evaluasi tersebut ditunjukkan pada Gambar 2.1 berikut.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Sumber (Hermawan et al., 2023).

Pada Gambar 2.1, persamaan matematis tersebut menjadi acuan dasar dalam menghitung nilai keberhasilan klasifikasi wajah terdaftar secara riil. Penerapan rumus evaluasi ini sangat krusial untuk memastikan hasil pengujian dari confusion matrix dapat dikonversikan menjadi persentase kinerja yang valid dan terukur. Berdasarkan kalkulasi parameter tersebut, model MobileFaceNet yang diimplementasikan pada perangkat komputasi dinyatakan sangat layak untuk mendukung otomatisasi pengenalan wajah pengguna karena memiliki tingkat presisi dan akurasi yang tinggi (Hermawan et al., 2023).

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB III
METODE PENELITIAN

3.1 Rancangan Penelitian

Penelitian ini menggunakan pendekatan penelitian kuantitatif yang dipilih karena evaluasi terhadap sistem keamanan biometrik yang dibangun menitikberatkan pada pengukuran kinerja secara objektif yang menghasilkan data numerik. Parameter terukur yang menjadi fokus utama dalam pendekatan ini meliputi nilai persentase akurasi klasifikasi identitas, tingkat kesalahan (*error rate*) pada pengujian biometrik biometrik, serta waktu latensi pemrosesan komputasi (*inference time*) lokal saat mengeksekusi fitur keaktifan wajah secara waktu-nyata (*real-time*).

Jenis penelitian yang diterapkan dalam pengerjaan skripsi ini adalah Riset Eksperimental sebab penelitian ini dilakukan dengan cara merancang, membangun, dan mengimplementasikan *prototype* sistem kontrol akses keamanan *smart door lock* berbasis perangkat *embedded* Raspberry Pi 4 Model B sebagai unit pemroses utama. Setelah *prototype* berhasil dibangun, eksperimen dilakukan di dalam lingkungan terkendali dengan memberikan berbagai skenario perlakuan, seperti melakukan pengujian pada variasi intensitas pencahayaan lingkungan yang berbeda (normal, *low-light*, dan *backlight*) serta pengujian jenis *presentation attack*. Hal ini bertujuan untuk mengamati hubungan sebab-akibat serta dampak anomali pencahayaan dan rekayasa visual terhadap stabilitas ekstraksi geometri wajah serta ketangguhan sistem dalam mengklasifikasikan objek asli (*live subject*) maupun serangan pemalsuan (*spoofing attack*).

Pengumpulan data pada penelitian ini dilakukan melalui pengukuran empirik atau observasi perangkat keras dan perangkat lunak secara langsung saat sistem beroperasi melalui dua jalur pemrosesan citra yang terpisah.

Data biometrik (geometri 468 titik *landmark* wajah dari MediaPipe Face Mesh dan identitas dari MobileFaceNet) diperoleh melalui perekaman log koordinat serta *dataset* wajah asli manusia hidup (*live subject*), yang diproses secara eksklusif menggunakan citra perbaikan (*enhanced frame*) hasil normalisasi algoritma CLAHE.

© Hak Cipta milik Politeknik Negeri Jakarta

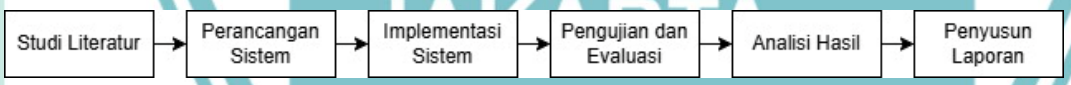
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Data penilaian cahaya dan metrik kinerja sistem dikumpulkan dengan mengekstrak nilai rata-rata luminans pada citra mentah (*raw frame*) asli sebelum proses peningkatan kontras, serta merekam *timestamp* internal program untuk mengukur waktu komputasi (milidetik) hingga pin GPIO mengaktifkan *solenoid door lock*.

Data metrik yang telah dikumpulkan dari berbagai skenario pengujian kemudian dianalisis menggunakan teknik analisis deskriptif kuantitatif. Seluruh data hasil pengukuran nilai *Accuracy*, *False Acceptance Rate* (FAR), *False Rejection Rate* (FRR), dan waktu tempuh komputasi akan dikumpulkan, dianalisa, dan divisualisasikan dalam bentuk grafik atau tabel komparasi. Melalui analisis ini, akan dievaluasi secara komprehensif apakah pemisahan alur penilaian cahaya pada citra mentah serta implementasi algoritma CLAHE dan *liveness detection* interaktif yang diterapkan pada arsitektur *edge computing* Raspberry Pi mampu menjawab tantangan integritas keamanan pada sistem pengenalan wajah konvensional dari ancaman serangan *spoofing*.

3.2 Tahapan Penelitian

Pelaksanaan penelitian ini dilakukan secara sistematis dan terstruktur melalui beberapa tahapan yang berkesinambungan. Alur metodologi ini dirancang untuk memastikan pembangunan sistem berjalan sesuai rencana dan dapat divalidasi kinerjanya dengan baik. Secara garis besar, tahapan pelaksanaan penelitian ditunjukkan pada Gambar berikut.



Gambar 3. 1 Tahapan Penelitian

Gambar 3.1 memperlihatkan tahapan pelaksanaan penelitian yang diawali dengan studi literatur untuk memperkuat landasan teori sistem keamanan biometrik wajah. Tahap berikutnya adalah perancangan sistem untuk merancang arsitektur *smart door lock*, spesifikasi pemisahan alur citra (*raw* dan *enhanced frame*), serta modul *liveness detection*. Rancangan tersebut direalisasikan melalui tahap implementasi sistem pada perangkat *embedded* Raspberry Pi 4 Model B, kemudian divalidasi kinerjanya pada tahap pengujian dan evaluasi di bawah variasi kondisi pencahayaan dan skenario serangan *spoofing*. Data metrik yang terkumpul selanjutnya masuk ke

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

tahap analisis hasil secara mendalam untuk mengukur parameter akurasi, FAR, FRR, serta latensi komputasi, sebelum akhirnya didokumentasikan secara utuh pada tahap penyusunan laporan.

3.3 Objek Penelitian

Objek utama yang dikaji dalam penelitian ini adalah mekanisme kontrol akses keamanan biometrik wajah berbasis arsitektur *edge computing* yang diimplementasikan pada sistem penguncian pintu pintar (*smart door lock*) dengan pemisahan alur pemrosesan citra digital untuk optimalisasi deteksi keaktifan (*liveness detection*). Mekanisme tersebut diterapkan pada studi kasus sistem pengamanan ruangan laboratorium komputer menggunakan komputer papan tunggal (*Single Board Computer*) Raspberry Pi, yaitu Raspberry Pi 4 Model B, yang dipilih berdasarkan kesesuaian karakteristik teknis serta kapabilitas komputasi lokalnya yang mumpuni dalam mengeksekusi algoritma *computer vision* secara waktu-nyata (*real-time*).

Subjek uji coba yang dilibatkan dalam penelitian ini berjumlah 30 data wajah, terdiri dari 16 data wajah perempuan dan 14 data wajah laki-laki, dengan variasi usia yang beragam, mulai dari anak-anak, remaja, dewasa, hingga lanjut usia (kakek/nenek). Variasi usia pada data wajah yang beragam ini turut merepresentasikan keberagaman karakteristik geometri dan tekstur wajah yang diujikan pada sistem.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB IV
HASIL DAN PEMBAHASAN

4.1 Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk mengidentifikasi spesifikasi sistem yang diperlukan dalam penelitian rancang bangun sistem pengenalan wajah dengan *liveness detection* sebagai mekanisme *anti-spoofing* pada arsitektur *edge computing* Raspberry Pi. Analisis ini dibagi menjadi empat bagian utama, yaitu kebutuhan fungsional, non-fungsional, perangkat keras, dan perangkat lunak.

4.1.1 Analisis Kebutuhan Perangkat Keras (*Hardware*)

Kebutuhan perangkat keras dalam penelitian ini ditentukan berdasarkan arsitektur sistem yang dikembangkan, yaitu sistem kontrol akses keamanan *smart door lock* terintegrasi berbasis perangkat *edge computing device*. Sistem terdiri dari dua komponen utama, yaitu unit pemroses citra (*edge computing*) dan unit kontrol aktuator fisik.

4.1.1.1 Unit Pemroses Citra (*Edge Computing Unit*)

Unit pemroses citra bertindak sebagai core processor lokal yang menangani seluruh alur data visual secara *real-time*. Komponen di dalam unit ini berfungsi untuk menangkap aliran video streaming melalui sensor optik kamera, memetakan topologi wajah, mengeksekusi algoritma *liveness detection*, hingga mengelola antarmuka grafis (GUI) secara langsung pada layar monitor portable mini. Seluruh proses komputasi berat tersebut dilakukan secara *on-device* tanpa bergantung pada server luar demi memangkas latensi respons. Komponen-komponen perangkat keras pada unit pemroses citra ini dapat dilihat spesifikasinya pada Tabel 4.1 berikut:

Tabel 4.1 Hardware Unit Pemroses Citra

No	Nama Komponen	Spesifikasi
1.	Raspberry Pi 4 Model B (8GB)	- Prosesor: Broadcom BCM2711, Quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz. - Memori: 8 GB LPDDR4-3200 SDRAM.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Nama Komponen	Spesifikasi
		- Konektivitas: 2.4 GHz dan 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE. - Antarmuka: 40-pin GPIO *header* - Port Daya: 5V DC via konektor USB-C (minimum 3A).
2.	Kamera USB (Webcam)	- Tipe: Digital Video Camera. - Resolusi Citra: High Definition (HD 720p / 1080p). - Antarmuka: USB 2.0 / USB 3.0 *Plug-and-Play.* - *Frame Rate*: Hingga 30 FPS - Sudut Pandang (*Field of View*): 60 – 90 Derajat.
3	LCD TFT Raspberry Pi 3.5	- Ukuran Layar: 3.5 Inch - Tipe Panel: TFT Touchscreen - Resolusi: 480 x 320 Piksel - Antarmuka Kontrol: SPI (Dihubungkan langsung ke pin GPIO) - Tingkat Refresh Rate: Hingga 50Hz / 60Hz FPS

4.1.1.2 Unit Kontrol dan Aktuator Fisik (*Actuator & Interface Unit*)

Perangkat kontrol dan aktuator berfungsi untuk mengubah sinyal perintah digital dari unit pemroses menjadi tindakan mekanis berupa penguncian fisik pintu, meregulasi distribusi tegangan listrik tinggi agar aman dikonsumsi perangkat mikro, serta menyediakan antarmuka tombol interaksi manual bagi pengguna dari dalam ruangan. Unit ini menjembatani arus komputasi bertegangan rendah dengan arus beban induktif sirkuit pengunci magnetik melalui sistem saklar isolasi

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

elektronik. Komponen-komponen perangkat keras pada unit kontrol dan aktuator fisik ini dapat dilihat spesifikasinya pada Tabel 4.2 berikut:

Tabel 4.2 Hardware Unit Kontrol dan Aktuator Fisik

No	Nama Komponen	Spesifikasi
1	Solenoid Door Lock 12V	- Tegangan Kerja: 12 VDC. - Arus Kerja: 0.6 A – 1.2 A - Material: Besi / Baja Anti Karat. - Jenis Kunci: *Fail-Secure* (Terkunci rapat saat arus mati). - Panjang Lidah Kunci: 10 mm.
2	Modul Relay 1 Channel	- Tegangan Pemicu (VCC): 5 VDC. - Tegangan Kontak Maksimum: 250 VAC / 30 VDC. - Arus Kontak Maksimum: 10 A. - Konfigurasi Output: NO (*Normally Open*), NC (*Normally Closed*), COM. - Tipe Pemicu: *High-Level Trigger.*
3	Push Button (Self-Reset)	- Tipe: *Momentary Switch (Self-Reset via Internal Spring)*. - Konfigurasi Kontak: SPST (*Single Pole Single Throw*), NO (*Normally Open*).

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Nama Komponen	Spesifikasi
		- Jenis Antarmuka: 2-Pin Header terhubung langsung ke pin GPIO lokal. - Nilai Tegangan Kerja: Maksimal 12V - 24V DC. - Karakteristik Otomasi: Memutus kontak kembali secara instan setelah tekanan dilepas.
4	Modul Stepdown DC-DC (LM2596)	- Tipe: Non-isolated buck module. - Tegangan Input: 4.5 V – 40 VDC. - Tegangan Output: Diatur pada 5 VDC (Adjustable via Potentiometer). - Arus Output: Maksimal 3A (Aman untuk menyuplai Raspberry Pi 4). - Efisiensi Konversi: Hingga 92%.
5	Adaptor Daya 12V	- Tegangan Input: 100-240 VAC, 50/60 Hz. - Tegangan Output: 12 VDC. - Arus Output Maksimum: 3 A – 5 A. - Tipe Konektor: DC Jack 5.5mm / Jalur Kabel Terbuka.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.1.2 Analisis Kebutuhan Perangkat Lunak

Kebutuhan perangkat lunak dalam penelitian ini mencakup seluruh komponen sistem yang mendukung implementasi pemrosesan citra wajah, ekstraksi geometri titik *landmark*, mekanisme *liveness detection* (*head pose* dan *blink*), klasifikasi biometrik, serta pengelolaan penyimpanan data berbasis lokal dan *cloud*. Lebih lanjut, perangkat lunak yang dibutuhkan dalam penelitian ini dijelaskan pada tabel 4.3 berikut:

Tabel 4.3 Kebutuhan Perangkat Lunak

No	Perangkat Lunak	Fungsi
1	Python 3.9.6	Bahasa pemrograman utama untuk mengembangkan seluruh arsitektur dan logika sistem, mengendalikan pin GPIO menuju relay, mengintegrasikan pustaka kecerdasan buatan, serta mengelola alur eksekusi data secara lokal.
2	OpenCV (*Open Source Computer Vision Library*)	Pustaka pemrosesan citra digital yang berfungsi untuk menangkap aliran video (*video stream*) dari modul kamera, melakukan manipulasi matriks gambar, serta mendukung visualisasi antarmuka pemindaian wajah.
3	MediaPipe FaceMesh	*Framework open-source* berbasis *deep learning* yang berfungsi untuk mendeteksi keberadaan wajah secara *real-time* serta mengekstraksi 468 titik koordinat *landmark* tiga dimensi (3D) dari bingkai citra digital.
4	Modul *Liveness Detection* (*Head Pose & Blink*)	Komponen algoritma yang berfungsi untuk menganalisis data spasial-temporal dari koordinat *landmark* wajah guna menghitung nilai *Eye Aspect Ratio* (EAR) untuk deteksi kedipan mata serta sudut rotasi kepala sebagai mekanisme *anti-spoofing*.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Perangkat Lunak	Fungsi
5	Model AI *MobileFaceNet*	Arsitektur jaringan saraf konvolusional (*Convolutional Neural Network*) ringan yang dioptimalkan untuk mengekstrak fitur karakteristik wajah (*face embedding*) dan menghitung skor *cosine similarity* untuk pencocokan identitas secara lokal.
6	SQLite Database	Sistem manajemen basis data relasional lokal yang tertanam secara mandiri di dalam penyimpanan Raspberry Pi untuk menyimpan data enkripsi *embedding* wajah pengguna sah agar dapat diakses dengan cepat tanpa ketergantungan internet.
7	Supabase Database Cloud	Platform basis data berbasis cloud (PostgreSQL) yang berfungsi untuk mencatat dan menyimpan log riwayat aktivitas akses pintu (*access logs*) secara asinkron untuk kebutuhan pemantauan data dari jarak jauh.

4.1.3 Analisis Kebutuhan Fungsional dan Non-Fungsional

Analisis kebutuhan sistem bertujuan untuk mengidentifikasi kebutuhan yang harus dipenuhi agar sistem yang dikembangkan dapat beroperasi sesuai dengan tujuan penelitian. Kebutuhan sistem pada penelitian ini dibagi menjadi kebutuhan fungsional dan kebutuhan non-fungsional.

4.1.3.1 Kebutuhan Fungsional

Kebutuhan fungsional mendefinisikan layanan atau fungsi yang harus dimiliki oleh sistem. Pada penelitian ini, kebutuhan fungsional difokuskan pada fungsi pengenalan wajah, implementasi mekanisme *liveness detection*, kontrol aktuator fisik, serta pengelolaan log data akses. Lebih lanjut, kebutuhan fungsional dari sistem ini dijelaskan pada tabel 4.4 berikut:

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.4 Kebutuhan Fungsional

No	Kebutuhan Fungsional
1	Sistem mampu menangkap aliran video (*video stream*) secara *real-time* dari modul kamera.
2	Sistem mampu mendeteksi keberadaan wajah manusia dan mengekstraksi titik *landmark* tiga dimensi (3D) dari citra visual.
3	Sistem mampu memberikan tantangan gerakan acak (*challenge-response*) kepada pengguna, seperti menoleh, mengangguk, atau berkedip untuk proses validasi.
4	Sistem mampu melakukan verifikasi keaktifan wajah (*liveness detection*) untuk membedakan wajah manusia asli dengan media pemalsuan (*spoofing*) berupa foto cetak atau video.
5	Sistem mampu mengekstrak fitur *embedding* wajah dan mencocokkannya dengan data identitas pengguna yang telah terdaftar di dalam basis data lokal.
6	Sistem mampu mengirimkan sinyal digital (pemicu *relay*) untuk membuka kunci *solenoid door lock* secara otomatis apabila proses autentikasi wajah berhasil dan lolos uji keaktifan.
7	Sistem mampu mencatat dan mengirimkan log riwayat aktivitas akses (meliputi waktu, identitas, tingkat akurasi, dan kondisi cahaya) ke dalam *database cloud* Supabase.
8	Sistem memiliki mode operasi pendaftaran (*register*) untuk merekam dan menambahkan data fitur wajah pengguna baru ke dalam basis data.

4.1.3.2 Kebutuhan Non-Fungsional

Kebutuhan non-fungsional merupakan atribut kualitas yang menentukan perilaku, kinerja, keamanan, dan keandalan sistem, hal ini mencakup kecepatan, skalabilitas, dan kenyamanan pengguna, serta memastikan sistem beroperasi dengan baik. Kebutuhan non-fungsional dari penelitian ini dijelaskan pada tabel 4.5 berikut:

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.5 Kebutuhan Non-Fungsional

No	Kebutuhan Non-Fungsional
1	Proses komputasi *face recognition* dan *liveness detection* harus memiliki waktu respons (*inference time*) yang cepat agar sistem berjalan secara *real-time* di perangkat *edge computing* Raspberry Pi.
2	Sistem harus tetap andal dan akurat dalam mendeteksi wajah pada berbagai kondisi pencahayaan yang dinamis (kondisi normal, *low-light*, maupun *backlight*).
3	Proses autentikasi dan ekstraksi fitur biometrik wajib diproses sepenuhnya secara lokal (*on-device processing*) guna menjamin privasi dan keamanan data pengguna dari risiko peretasan jaringan.
4	Sistem harus mampu mereset status tahapan verifikasi secara otomatis (*state machine reset*) apabila wajah pengguna tiba-tiba menghilang dari jangkauan kamera untuk mencegah akses tidak sah.
5	Sistem tidak akan mengganggu kinerja pemrosesan aliran video saat sedang melakukan pengiriman data log ke cloud, sehingga tampilan streaming tidak mengalami lag.

4.2 Perancangan Sistem

Tahap perancangan sistem dalam penelitian ini bertujuan untuk memodelkan integrasi arsitektur perangkat keras dan perangkat lunak dalam membangun mekanisme kontrol akses pintu pintar (*smart door lock*) berbasis kecerdasan buatan (*Artificial Intelligence*) dan *Internet of Things* (IoT). Sebagai studi kasus, mekanisme keamanan ini diaplikasikan pada pengamanan ruangan fisik yang memanfaatkan modul kamera untuk membaca fitur biometrik wajah. Oleh karena itu, desain sistem secara keseluruhan dirancang agar mampu mengakomodasi dua fungsi utama secara simultan, yakni memproses ekstraksi fitur wajah dan *liveness detection* secara lokal (*on-device processing*) dengan tingkat latensi yang rendah,

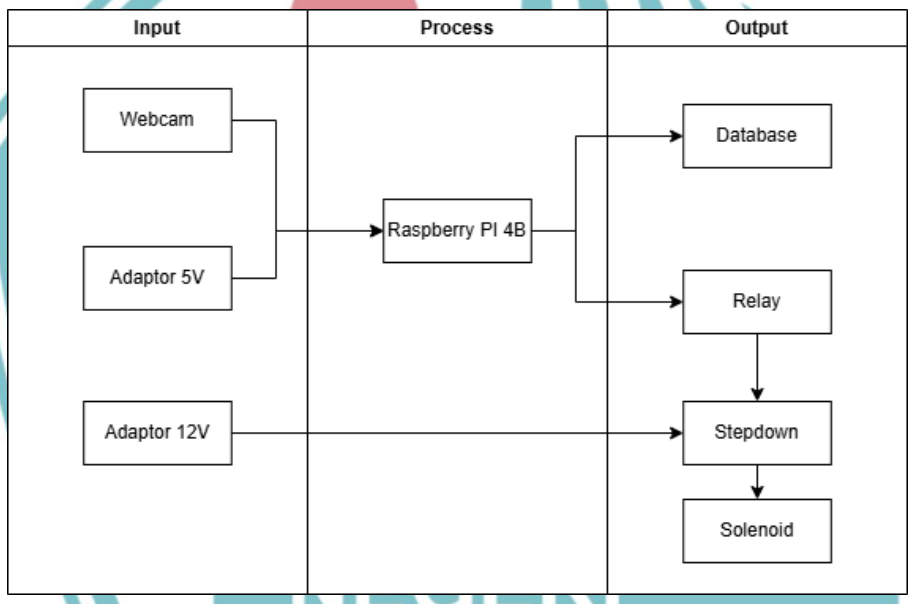
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

sekaligus memfasilitasi jalur pencatatan log riwayat akses secara *real-time* ke sistem *cloud* tanpa mengganggu kinerja utama perangkat keras.

4.2.1 Blok Diagram

Perancangan perangkat keras pada sistem ini dibagi menjadi tiga bagian utama, yaitu komponen masukan (*input*), unit pemroses (*process*), dan komponen keluaran (*output*). Pembagian ini bertujuan untuk memetakan alur kerja data serta distribusi daya listrik antarkomponen secara terstruktur. Secara keseluruhan, konfigurasi dan interkoneksi antarkomponen sistem tersebut ditunjukkan secara detail pada Gambar 4.1 berikut.



Gambar 4. 1 Blok Diagram

Berdasarkan struktur yang ditunjukkan pada Gambar 4.1 di atas, interaksi antarkomponen dalam sistem terbagi secara sistematis ke dalam tiga kolom utama. Pada bagian *input*, terdapat Webcam sebagai sensor penangkap citra visual dan Adaptor 5V yang berfungsi memasok daya utama ke unit pemroses, serta Adaptor 12V yang bertindak sebagai sumber daya eksternal untuk sistem pengunci elektrik. Bagian *process* sepenuhnya dikendalikan oleh Raspberry Pi 4B sebagai pusat pemrosesan data utama yang menerima masukan data dari webcam dan suplai daya dari adaptor 5V. Selanjutnya, pada bagian *output*, Raspberry Pi 4B terhubung ke Database untuk sinkronisasi data sekaligus mengirimkan sinyal kendali ke modul Relay. Dari aspek kelistrikan beban, aliran daya dari Adaptor 12V dikirimkan

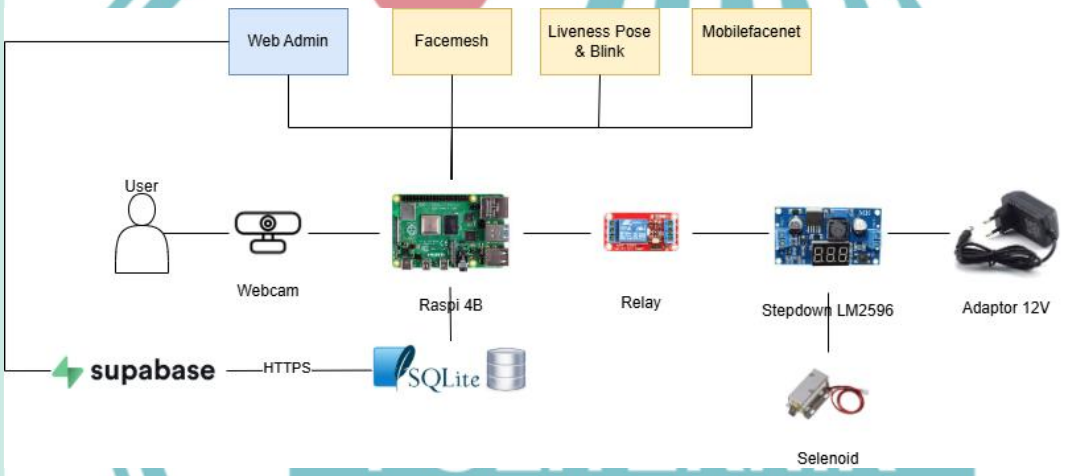
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

menuju modul penurunan tegangan atau Stepdown, di mana modul ini dikontrol secara aktif oleh Relay untuk menentukan kapan arus listrik diteruskan guna mengaktifkan kunci pintu elektronik atau Solenoid ketika akses dinyatakan valid oleh sistem.

4.2.2 Arsitektur Sistem

Perancangan arsitektur sistem dilakukan untuk memetakan hubungan integrasi antarkomponen perangkat keras, modul kecerdasan buatan (*Artificial Intelligence*), dan manajemen basis data (*database*) yang saling tersinkronisasi. Struktur interkoneksi global serta alur fungsionalitas dari sistem keamanan akses ini secara detail ditunjukkan pada Gambar 4.2 berikut.



Gambar 4. 2 Arsitektur Sistem

Berdasarkan struktur yang ditunjukkan pada Gambar 4.2 di atas, sistem ini beroperasi melalui dua proses utama, yaitu registrasi dan check-in. Pada proses registrasi, admin mendaftarkan pengguna via Web Admin yang memicu Raspberry Pi dan Webcam untuk mengambil data wajah, lalu mengekstraksinya menggunakan modul AI FaceMesh, Liveness Pose & Blink, serta MobileFaceNet sebelum disimpan ke lokal SQLite dan disinkronkan ke cloud Supabase melalui jalur HTTPS. Sementara pada proses check-in, Webcam menangkap wajah pengguna untuk diverifikasi oleh Raspberry Pi menggunakan model AI yang sama jika identitas valid, Raspberry Pi mengaktifkan modul Relay untuk mengalirkan daya dari step-down converter menuju Solenoid agar pintu terbuka. Setiap riwayat akses masuk tersebut otomatis tercatat ke dalam SQLite sebagai access log, kemudian

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

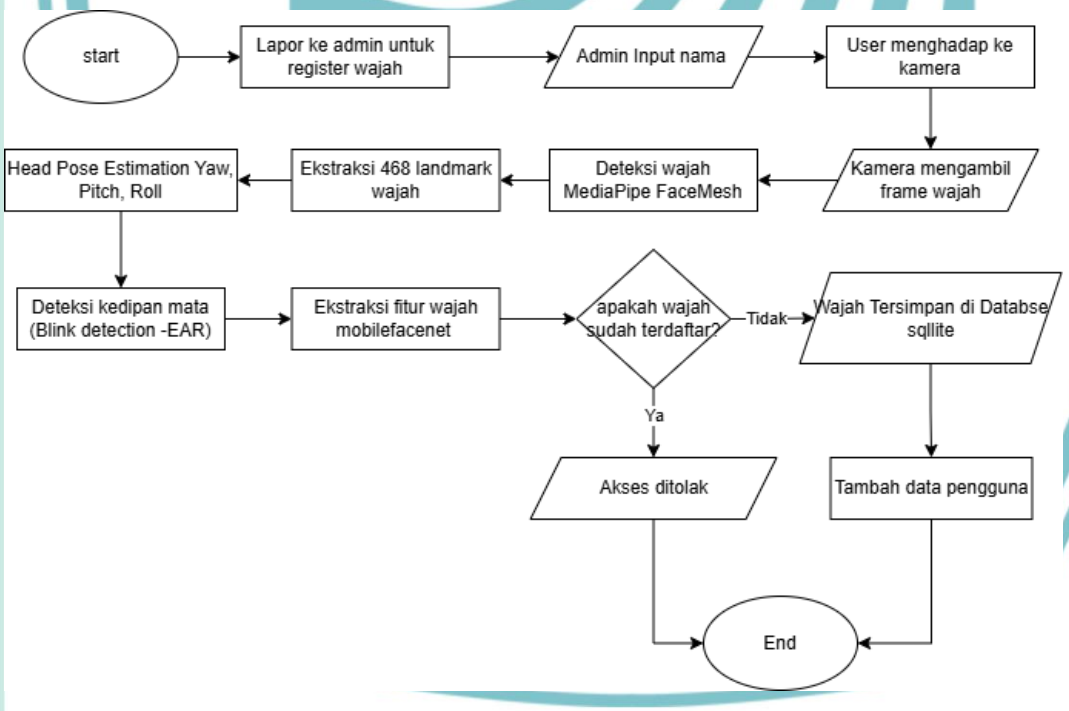
ditransmisikan ke Supabase via HTTPS sehingga data pemantauan dapat langsung diakses secara terpusat oleh admin melalui halaman Web Admin.

4.2.3 Diagram Alir

Rancangan logika pemrograman pada sistem *smart door lock* ini dimodelkan menggunakan diagram alir (*flowchart*) yang terbagi menjadi dua proses utama, yaitu proses pendaftaran pengguna baru *(Register)* dan proses pencocokan identitas (Pengenalan Wajah).

4.2.3.1 Diagram Alir Proses Pendaftaran (*Register*)

Perancangan diagram alir ini dilakukan untuk menggambarkan urutan instruksi dan logika sistem saat mendeteksi serta mendaftarkan karakteristik biometrik wajah pengguna baru. Alur sistematis dari proses registrasi tersebut ditunjukkan secara detail pada Gambar 4.3 berikut.



Gambar 4. 3 Diagram Alir Proses Pendaftaran

Berdasarkan alur yang ditunjukkan pada Gambar 4.3 di atas, proses pendaftaran diawali dengan input nama oleh *administrator*, dilanjutkan pengambilan citra wajah melalui kamera yang langsung diproses oleh MediaPipe FaceMesh untuk mengekstraksi 468 titik *landmark*. Titik tersebut diuji melalui modul *liveness detection* berdasarkan estimasi pergerakan kepala (*yaw, pitch, roll*) dan kedipan

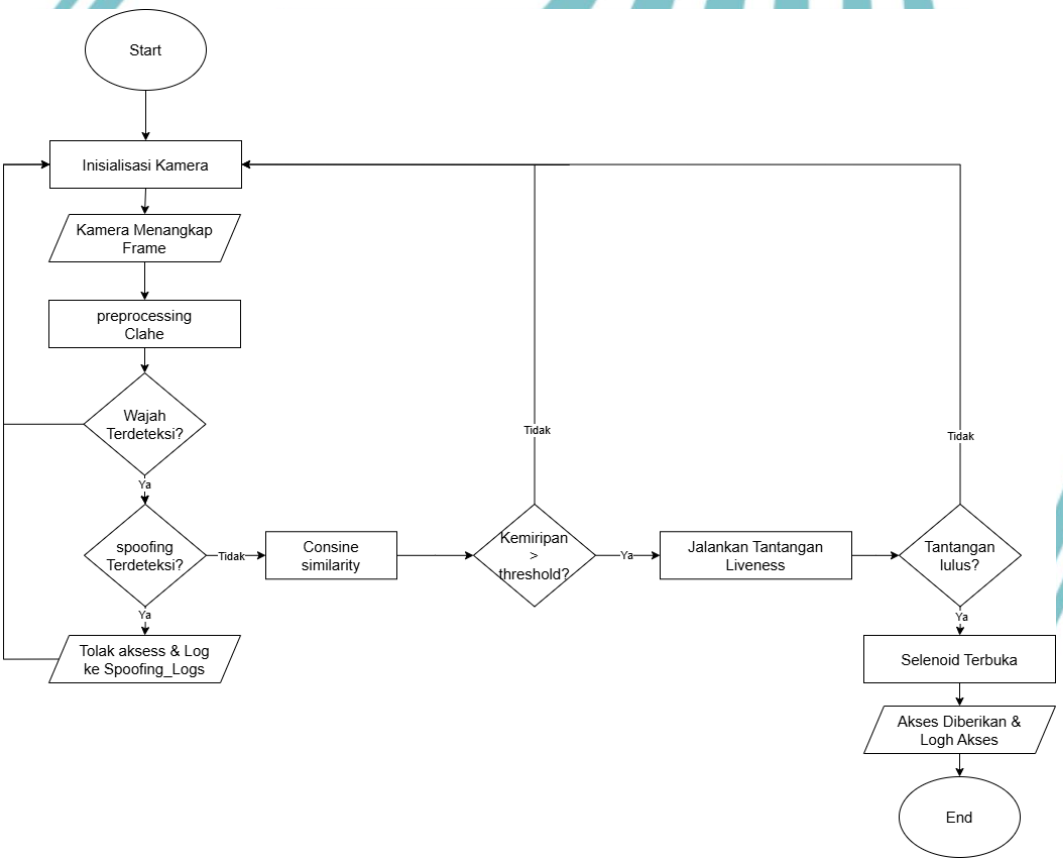
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

mata (*Eye Aspect Ratio*/EAR) demi menjamin keaslian subjek. Jika lolos uji keaktifan, fitur biometrik wajah akan diekstrak menggunakan MobileFaceNet untuk dilakukan validasi duplikasi; apabila wajah sudah terdaftar maka pendaftaran otomatis dibatalkan dengan luaran "*Akses Ditolak*", namun jika data wajah bersifat unik (belum ada di sistem), identitas dan fitur biometrik tersebut akan langsung disimpan ke dalam basis data SQLite sebagai pengguna baru.

4.2.3.2 Diagram Alir Proses Verifikasi (Pengenalan Wajah)

Perancangan diagram alir ini dilakukan untuk menggambarkan logika dan urutan instruksi sistem saat melakukan pemindaian, perbaikan kualitas citra, verifikasi identitas, hingga pengambilan keputusan akses pintu. Alur sistematis dari proses verifikasi tersebut ditunjukkan secara detail pada Gambar 4.4 berikut.



Gambar 4. 4 Diagram Alir Proses Verifikasi

Berdasarkan alur yang ditunjukkan pada Gambar 4.4 di atas, proses verifikasi diawali dengan penangkapan citra wajah oleh kamera yang langsung dinormalisasi menggunakan algoritma CLAHE, lalu dipindai oleh MediaPipe FaceMesh (jika wajah tidak terdeteksi, sistem akan mengulang pengambilan gambar). Apabila

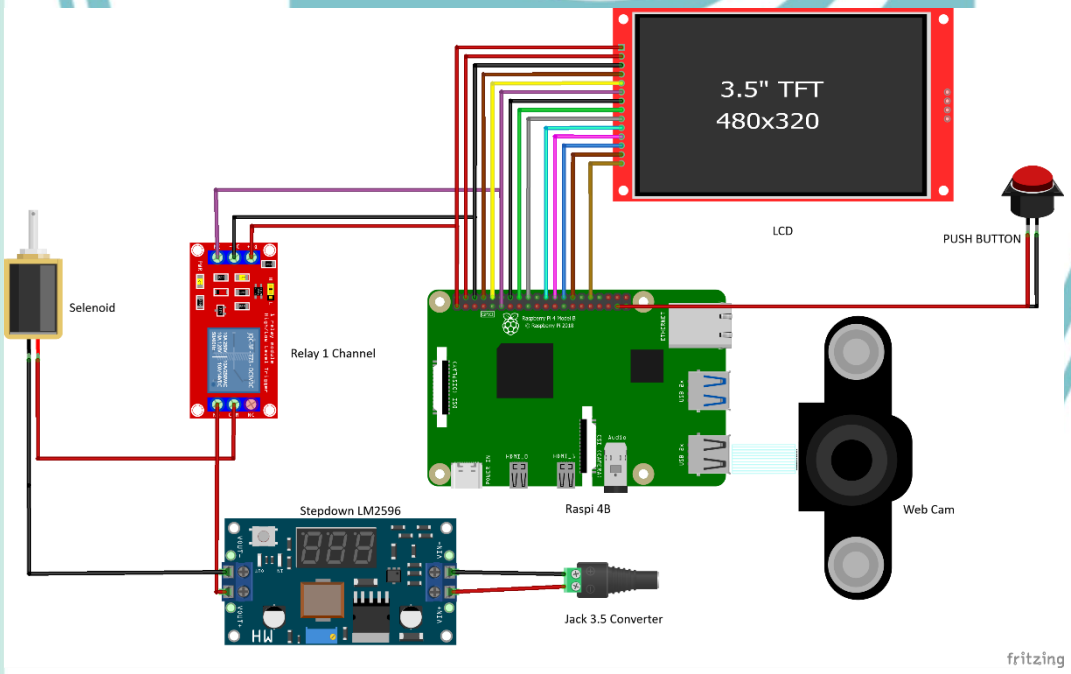
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

wajah terdeteksi namun basis data lokal SQLite kosong, sistem akan memicu *State Error* dan menghentikan program; namun jika data tersedia, model MobileFaceNet akan mengekstrak fitur wajah untuk dihitung kemiripannya menggunakan metode *Cosine Similarity*. Pengguna yang memiliki skor di bawah ambang batas (*threshold*) atau gagal dalam tantangan keaktifan (*liveness challenge*) otomatis ditolak aksesnya dan *log* kegagalan dikirim ke *cloud* Supabase. Sebaliknya, jika identitas dinyatakan valid dan lolos uji keaktifan, Raspberry Pi akan memicu modul Relay dan Stepdown untuk membuka kunci Solenoid, serta secara paralel mengirimkan *log* keberhasilan akses ke Supabase sebelum kembali ke status siaga (*idle*).

4.2.4 Rancangan Skematik Alat

Perancangan skematik rangkaian dilakukan untuk memetakan interkoneksi fisik, distribusi pin GPIO, serta sistem pengondisian daya antar-komponen elektronika. Konfigurasi pinout dan integrasi perangkat keras pada sistem ini ditunjukkan secara detail pada Gambar 4.5 berikut.



Gambar 4. 5 Rancangan Skematik Alat

Berdasarkan konfigurasi pin dan interkoneksi pada Gambar 4.5 di atas, sistem ini mengintegrasikan seluruh komponen melalui empat subsistem utama sebagai berikut:

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

a) Subsistem Manajemen Daya

Sistem ini menggunakan dua sumber energi utama yang dipisahkan berdasarkan kebutuhan tegangan kerja masing-masing komponen. Untuk unit pemrosesan data, Raspberry Pi 4 mendapat suplai daya secara mandiri menggunakan Adaptor 5V bawaan (*official power supply*) melalui port USB Type-C guna menjaga stabilitas kinerja komputasi.

Sementara itu, sirkuit aktuator menggunakan Adaptor DC 12V terpisah sebagai sumber energi utama yang dihubungkan langsung menuju jalur masukan Modul *Stepdown* DC-DC (*Buck Converter*) pada pin IN+ (positif adaptor) dan IN- (negatif adaptor). Modul *stepdown* ini berfungsi menurunkan serta meregulasi tegangan dari 12V ke tingkat tegangan kerja yang dibutuhkan oleh *Solenoid Door Lock* agar dapat bergerak secara aman tanpa risiko panas berlebih (*overheat*). Jalur keluaran negatif (OUT-) dari *stepdown* dialirkan langsung menuju terminal negatif *Solenoid Door Lock*, sedangkan jalur keluaran positif (OUT+) dijembatani terlebih dahulu melalui modul relay pada pin *Normally Open* (NO) sebelum diteruskan ke beban terminal positif solenoid. Rincian konfigurasi jalur distribusi daya sistem ini dirangkum pada Tabel 4.6.

Tabel 4.6 Subsistem Manajemen Daya

Titik Asal	Pin/Jalur Asal	Titik Tujuan	Pin/Jalur Tujuan
Adaptor 5V Bawaan	USB Type-C	Raspberry Pi 4B	Port Daya Type-C
Adaptor 12V DC	Kutub Positif (+)	Modul Stepdown DC-DC	IN+
Adaptor 12V DC	Kutub Negatif (-)	Modul Stepdown DC-DC	IN-
Modul Stepdown DC-DC	OUT+ (Tegangan Regulasi)	Modul Relay 1-Channel	NO (*Normally Open*)
Modul Relay 1-Channel	COM (*Common*)	Solenoid Door Lock	Terminal Positif (+)
Modul Stepdown DC-DC	OUT-	Solenoid Door Lock	Terminal Negatif (-)

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

b) Subsistem Pengolahan Citra Visual

Sebagai unit akuisisi data biometrik, digunakan Modul Kamera / *Webcam* berbasis USB. Kamera ini membutuhkan *bandwidth* transfer data yang tinggi sehingga dikoneksikan langsung pada port USB 3.0 yang tersedia di sasis antarmuka Raspberry Pi 4. Pasokan daya untuk kamera diambil secara internal dari bus USB mikrokontroler. Hubungan antarmuka fisik untuk subsistem pengolahan citra visual ini dipaparkan pada Tabel 4.7.

Tabel 4.7 Subsistem Pengolahan Citra Visual

Titik Asal	Pin/Jalur Asal	Titik Tujuan	Pin/Jalur Tujuan
Kamera Webcam	Kabel Data USB	Raspberry Pi 4B	Port USB 3.0 / USB 2.0

c) Subsistem Antarmuka Visual (*Display Interface*)

Untuk memvisualisasikan petunjuk instruksi tantangan gerakan (*liveness challenge*), menampilkan pratinjau *streaming* kamera, serta memunculkan notifikasi status akses secara waktu-nyata kepada pengguna, digunakan modul LCD TFT 3.5 Inch. Komponen ini dipasang secara *shield* langsung di atas header GPIO 40-pin Raspberry Pi 4.

Protokol komunikasi data visual dikelola menggunakan bus SPI (*Serial Peripheral Interface*) kecepatan tinggi yang memanfaatkan pin utama MOSI, MISO, SCLK, serta pin kontrol logika *Chip Select* (CS), *Data/Command* (DC), dan *Reset* (RST). Kebutuhan daya operasional LCD disuplai langsung secara internal melalui pin daya 3.3V dan 5V Raspberry Pi. Pemetaan fungsional serta penomoran pin fisik untuk koneksi layar LCD TFT 3.5 Inch ini tertera pada Tabel 4.8.

Tabel 4.8 Subsistem Antarmuka Visual

Titik Asal	Fungsi Pin	Titik Tujuan	Pin / Jalur Tujuan (LCD TFT)
Pin 1 (3.3V Power)	Kutub Suplai Daya Logika	LCD TFT 3.5 Inch	VCC (3.3V)
Pin 2 (5V Power)	Suplai Daya Utama	LCD TFT 3.5 Inch	5V

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Titik Asal	Fungsi Pin	Titik Tujuan	Pin / Jalur Tujuan (LCD TFT)
Pin 6 (GND)	Common Ground	LCD TFT 3.5 Inch	GND
GPIO 10 (Pin 19)	SPI0 MOSI (Data Out)	LCD TFT 3.5 Inch	MOSI / DI
GPIO 9 (Pin 21)	SPI0 MISO (Data In)	LCD TFT 3.5 Inch	MISO / DO
GPIO 11 (Pin 23)	SPI0 SCLK (Clock)	LCD TFT 3.5 Inch	CLK / SCK
GPIO 8 (Pin 24)	SPI0 CE0 (*Chip Select*)	LCD TFT 3.5 Inch	CS
GPIO 25 (Pin 22)	Data / Command Select	LCD TFT 3.5 Inch	DC / RS
GPIO 24 (Pin 18)	Hardware Reset	LCD TFT 3.5 Inch	RST

d) Subsistem Aktuator dan Saklar Logika

Untuk mengeksekusi pembukaan pintu, digunakan Modul Relay 1-Channel bertenaga 5V yang dikendalikan melalui pin GPIO 18 pada Raspberry Pi 4. Modul relay bertindak sebagai saklar elektronik yang mengisolasi arus komputasi bertegangan rendah dengan arus beban induktif pada sirkuit pengunci. Ketika pin GPIO 18 menerima instruksi bernilai HIGH dari Raspberry Pi, medan magnet pada kumparan relay akan menarik tuas saklar internal sehingga pin *Normally Open* (NO) terhubung dengan pin *Common* (COM).

Kondisi sirkuit yang tertutup ini membuat tegangan regulasi dari OUT+ *stepdown* mengalir menuju terminal positif *Solenoid Door Lock*, sehingga grendel pintu secara fisik tertarik ke dalam. Detail pengabelan dan interkoneksi kendali logika aktuator ini dijabarkan pada Tabel 4.9.

Tabel 4.9 Subsistem Aktuator dan Saklar Logika

Titik Asal	Pin/Jalur Asal	Titik Tujuan	Pin/Jalur Tujuan
Raspberry Pi 4B	Pin 2 (5V Power)	Modul Relay 1-Channe	VCC

Titik Asal	Pin/Jalur Asal	Titik Tujuan	Pin/Jalur Tujuan
Raspberry Pi 4B	Pin 6 (GND)	Modul Relay 1-Channe	GND
Raspberry Pi 4B	GPIO 18 (Pin 12)	Modul Relay 1-Channe	IN / Signal

e) Subsistem Input Manual (*Push Button*)

Sebagai antarmuka tambahan untuk membuka kunci secara manual dari dalam ruangan, digunakan sebuah *push button* 2 kaki yang dirangkai menggunakan *breadboard*. Komponen ini bertindak sebagai pemicu input digital bagi mikrokontroler.

Satu kaki dari *push button* dihubungkan untuk membaca sinyal pada pin GPIO 26 (Pin 37) Raspberry Pi 4, sedangkan kaki lainnya dihubungkan ke salah satu titik *Ground* (Pin 39). Ketika tombol ditekan, status logika pada pin input akan berubah dan memberikan sinyal kepada sistem untuk mengaktifkan modul relay pembuka pintu. Konfigurasi pin kabel untuk tombol akses manual ini ditunjukkan pada Tabel 4.10.

Tabel 4.10 Subsistem Input Manual

Titik Asal	Pin/Jalur Asal	Titik Tujuan	Pin/Jalur Tujuan
Push Button 2 Kaki	Kaki / Terminal 1	Raspberry Pi 4B	GPIO 26 (Pin 37)
Push Button 2 Kaki	Kaki / Terminal 2	Raspberry Pi 4B	Ground (Pin 39)

4.2.5 Rancangan Basis Data

Rancangan basis data pada sistem ini menggunakan arsitektur penyimpanan ganda i(*hybrid storage architecture*) untuk menyimpan data pendaftaran biometrik pengguna, mencatat riwayat log akses, serta mendokumentasikan forensik upaya manipulasi (*spoofing*). Struktur data dirancang terdistribusi untuk menjamin integritas data melalui penerapan *Primary Key* (PK) dan *Foreign Key* (FK) yang terbagi antara basis data lokal *SQLite* dan *cloud PostgreSQL* (Supabase).

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.2.5.1 Rancangan Basis Data Lokal (SQLite)

Sistem memanfaatkan *SQLite* sebagai penyimpanan lokal (*RDBMS* ringan) di dalam *SD Card* Raspberry Pi 4B. Penyimpanan lokal ini bersifat *offline-first* yang krusial agar proses pencocokan biometrik dan inferensi kecerdasan buatan dapat dieksekusi secara instan tanpa hambatan latensi jaringan internet (*Input/Output*).

a) Entity Relationship Diagram (ERD) Lokal

Struktur tabel dan hubungan logika di dalam penyimpanan lokal Raspberry Pi 4B dimodelkan melalui diagram relasi entitas. Visualisasi struktur data lokal tersebut ditunjukkan pada Gambar 4.6 berikut.

Gambar 4. 6 Rancangan Basis Data SQLite

Berdasarkan Gambar 4.6, keterhubungan antar-tabel di sisi lokal diikat secara relasional menggunakan atribut user_id sebagai kunci relasi utama:

- Tabel registered_faces ke register_logs (One-to-Many): Satu data master pengguna dapat memiliki beberapa kali riwayat proses pendaftaran yang didokumentasikan pada tabel register_logs melalui foreign key user_id.
- Tabel registered_faces ke access_logs (One-to-Many): Satu data master pengguna (registered_faces) yang diidentifikasi berdasarkan kolom id dapat memiliki banyak rekam riwayat pemindaian akses masuk pada tabel access_logs melalui foreign key user_id.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

b) Mekanisme *Hybrid-Sync* dan Pengelolaan Data *Offline*

Untuk menjaga konsistensi data ketika sistem berjalan tanpa koneksi internet (*offline mode*), arsitektur *SQLite* pada penelitian ini mengimplementasikan dua komponen pelacak sinkronisasi khusus:

- Kolom Penanda Status (is_synced): Setiap tabel utama pada SQLite memiliki kolom is_synced bertipe data Integer. Ketika pemindaian terjadi dalam kondisi offline, data transaksi baru tetap ditulis ke lokal dengan nilai status is_synced = 0. Begitu koneksi internet pulih, background service berbasis Python akan mendeteksi baris berstatus 0, mengunggahnya ke cloud, lalu mengubah nilainya menjadi 1 (tersinkronisasi)
- Tabel Pelacak Penghapusan (sync_deletes): Tabel mandiri yang hanya ada di sisi lokal untuk mencatat nama tabel (table_name) dan ID data (record_id) yang telah dihapus oleh administrator saat offline, sehingga aksi penghapusan tersebut dapat direplikasi secara akurat ke server cloud ketika jaringan kembali tersedia.

4.2.5.2 Rancangan Basis Data Cloud (Supabase PostgreSQL)

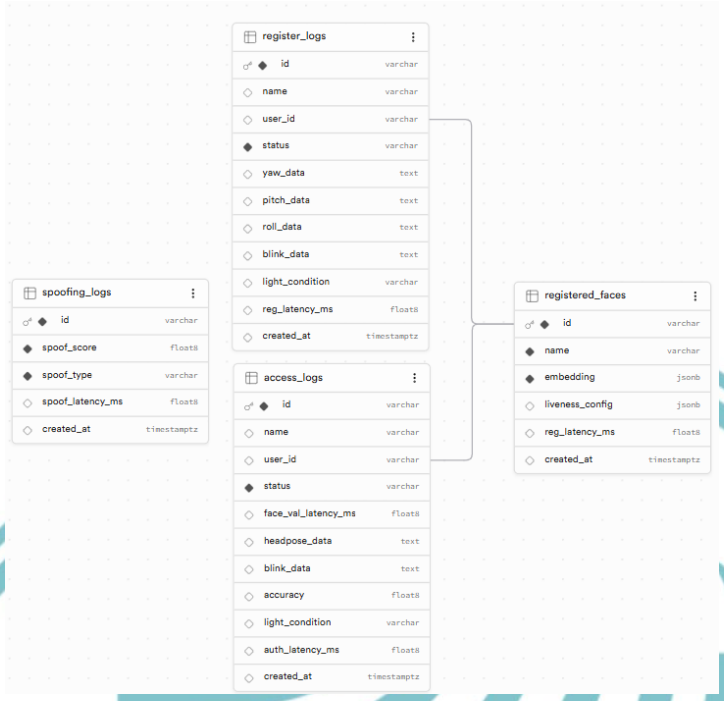
Untuk pelaporan telemetri, manajemen data terpusat, dan penyediaan sumber data utama dasbor *website monitoring* jarak jauh, sistem menggunakan *PostgreSQL* yang di-host melalui layanan *Supabase*.

a) Entity Relationship Diagram (ERD) Cloud

Hubungan logika antar-entitas makro pada sistem *cloud* dirancang untuk mendukung analisis forensik keamanan secara terstruktur. Arsitektur relasional pada *cloud storage* ini diilustrasikan pada Gambar 4.7 berikut.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4. 7 Rancangan Basis Data Supabase

Berdasarkan arsitektur *cloud* pada Gambar 4.7. relasi antar-tabel dihubungkan secara ketat menggunakan tipe data *user_id*:

- Tabel registered_faces ke access_logs (One-to-Many): Diikat oleh Foreign Key user_id pada tabel access_logs yang merujuk pada id unik pengguna sah di tabel master (registered_faces).
- Tabel registered_faces ke register_logs (One-to-Many): Log pendaftaran diikat oleh Foreign Key user_id pada tabel register_logs yang merujuk pada id di master data pengguna.
- Tabel spoofing_logs: Berdiri secara mandiri tanpa foreign key yang terikat ke tabel lain, berfungsi khusus untuk mencatat log aktivitas secara independen apabila sistem mendeteksi adanya serangan pemalsuan biometrik.

4.2.5.3 Deskripsi Fungsi Tabel Basis Data

Untuk mendukung arsitektur relasional terdistribusi yang telah dijabarkan di atas, fungsionalitas dan peran spesifik dari masing-masing entitas didefinisikan pada Tabel 4.11 berikut:

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.11 Deskripsi Fungsi Tabel Basis Data

No	Nama Tabel	Lokasi Penyimpanan	Deskripsi Fungsional Utama
1	access_logs	*SQLite* (Lokal) & *Supabase* (*Cloud*)	Berfungsi sebagai perekam data aktivitas harian pada pintu pintar. Setiap kali ada pengguna yang memindai wajah di depan kamera, tabel ini mencatat keputusan akhir sistem (*SUCCESS/FAILED*), tingkat kemiripan (*accuracy*), durasi latensi komputasi, serta kondisi pencahayaan untuk kebutuhan audit forensik keamanan.
2	registered_faces	*SQLite* (Lokal) & *Supabase* (*Cloud*)	Bertindak sebagai direktori atau buku induk identitas resmi pengguna sah (Nama & NIM). Tabel ini menyimpan nilai koordinat karakteristik wajah (*vector embedding*) hasil ekstraksi model *MobileFaceNet* serta parameter ambang batas gerakan kepala dan mata (*liveness config*) sebagai acuan utama verifikasi.
3	register_logs	*SQLite* (Lokal) & *Supabase* (*Cloud*)	Berfungsi untuk mendokumentasikan sejarah jalannya proses pendaftaran wajah baru oleh administrator. Tabel ini merekam kualitas data sensor visual (sudut

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Nama Tabel	Lokasi Penyimpanan	Deskripsi Fungsional Utama
			putaran kepala, kedipan mata, dan intensitas cahaya) serta waktu tunda (*latency*) komputasi dari awal registrasi hingga data berhasil disimpan secara permanen.
4	spoofing_logs	*SQLite* (Lokal) & *Supabase* (*Cloud*)	Dirancang khusus sebagai kotak hitam (*black box*) keamanan untuk mencatat aksi manipulasi biometrik wajah (*presentation attack*) yang berhasil digagalkan (seperti penggunaan foto cetak atau video). Tabel ini merekam nilai probabilitas kecurangan (*spoofing score*), kategori media pemalsuan, dan stempel waktu aktual serangan.
5	sync_deletes	*SQLite* (Eksklusif Lokal)	Berfungsi sebagai antrean memori sementara untuk menampung instruksi penghapusan data secara *offline*. Ketika admin menghapus hak akses pengguna saat perangkat kehilangan internet, tabel ini mencatat indeksnya, lalu secara otomatis memandu server *cloud* Supabase untuk ikut menghapus data tersebut

No	Nama Tabel	Lokasi Penyimpanan	Deskripsi Fungsional Utama
			begitu koneksi internet kembali pulih.

4.3 Implementasi Sistem

Tahap implementasi sistem merupakan proses pemindahan atau realisasi praktis dari seluruh rancangan teori dan diagram arsitektur ke dalam wujud prototipe fisik serta program aplikasi yang siap pakai. Fokus utama pada tahapan ini mencakup perakitan seluruh komponen perangkat keras, penulisan kode program (perangkat lunak) menggunakan Python untuk menjalankan sistem secara lokal, serta penerapan sistem basis data hibrida untuk manajemen penyimpanan data. Melalui rangkaian proses ini, seluruh subsistem kontrol akses pintu pintar (*smart door lock*) disatukan menjadi sebuah perangkat IoT fungsional yang siap diuji kinerjanya secara riil di lapangan.

4.3.1 Implementasi Perangkat Keras

Implementasi perangkat keras merupakan tahap perakitan dan pengintegrasian seluruh komponen fisik sistem *smart door lock* ke dalam satu kesatuan struktur prototipe. Proses ini bertujuan untuk merealisasikan arsitektur kontrol akses berbasis *edge computing* yang aman, andal, dan dapat beroperasi secara *real-time* di lapangan. Berikut adalah dokumentasi aktual dari hasil implementasi dan tata letak mekanis seluruh komponen perangkat keras yang telah diintegrasikan pada pintu prototipe.

Gambar 4. 8 Implementasi Perangkat Keras

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan hasil perakitan fisik yang ditunjukkan pada Gambar 4.8, keseluruhan komponen sistem diatur dan ditempatkan secara terpusat pada sebuah papan panel kayu yang merepresentasikan struktur pintu geser. Di bagian tengah panel, komponen utama Raspberry Pi 4 Model B (8GB RAM) dipasang dengan aman di dalam wadah (*case*) akrilik pelindung, di mana bagian atasnya langsung dipasangkan LCD TFT 3.5 Inch yang menyala aktif menampilkan antarmuka grafis sistem. Tepat di atas monitor tersebut, sebuah Kamera USB (Webcam) dipasang menggunakan braket jepit hitam agar posisinya sejajar dan optimal untuk menangkap area wajah pengguna secara *real-time*. Pada sisi sebelah kanan panel, komponen manajemen daya dan kendali otomatis dirangkai berdekatan, yang memperlihatkan Adaptor Daya 12V sebagai sumber listrik utama sistem, Modul Stepdown DC-DC (LM2596) untuk menurunkan tegangan bagi mikrokontroler, serta Modul Relay 1 Channel sebagai saklar elektronik. Seluruh aliran arus listrik tersebut bermuara pada Solenoid Door Lock 12V yang terpasang di bagian bawah panel pintu untuk mengunci grendel secara mekanis. Sebagai pelengkap interaksi manual dari dalam ruangan, sebuah Push Button Self-Reset berwarna merah ditempatkan di sudut kanan atas panel dengan interkoneksi kabel jumper, yang berfungsi agar pengguna dapat membuka pengunci solenoid dan keluar ruangan secara instan hanya dengan sekali tekan.

4.3.2 Implementasi Perangkat lunak

Pengembangan perangkat lunak dibangun di atas bahasa pemrograman Python yang berjalan di lingkungan sistem operasi Linux Raspberry Pi. Pemrosesan algoritma kecerdasan buatan (*Deep Learning*) dijalankan sepenuhnya di sisi lokal (*edge computing*) menggunakan mesin inferensi *ONNX Runtime* terkompresi guna menekan waktu tunda (*latency*).

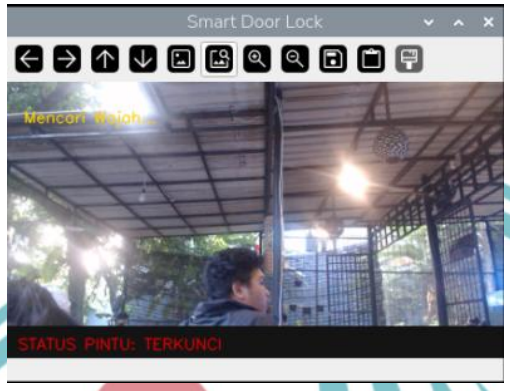
4.3.2.1 Tampilan Halaman Utama dan Inisialisasi Sistem

Sebelum sistem masuk ke dalam proses pendaftaran maupun pengenalan biometrik autentikasi, perangkat lunak akan memuat halaman utama sebagai kondisi siap pakai (*default state*). Antarmuka ini dirancang menggunakan resolusi native 480x320 piksel (mode *landscape*) agar dapat disajikan secara penuh (*fullscreen*) pada layar monitor LCD TFT 3.5 Inci yang terpasang pada perangkat keras

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Raspberry Pi. Antarmuka ini memuat indikator operasional awal untuk mendeteksi objek kamera serta melacak status pengunci fisik pintu secara berkelanjutan.



Gambar 4. 9 Tampilan Halaman Utama

Gambar 4.9 menunjukkan implementasi antarmuka halaman utama perangkat lunak saat sistem pertama kali diaktifkan. Pada tampilan awal operasional alat ini, sistem secara *real-time* menyajikan *live camera stream* pada area tengah layar untuk memantau objek di depan pintu. Tampilan tersebut memunculkan status teks "Mencari Wajah..." berwarna kuning di pojok kiri atas layar yang mengonfirmasi bahwa fungsionalitas penjejakan *landmark* wajah sedang aktif memindai area tangkapan secara berkelanjutan untuk menemukan objek biometrik. Sementara itu, bilah bar hitam di sisi paling bawah layar menampilkan informasi keamanan berupa teks "STATUS PINTU: TERKUNCI" berwarna merah mencolok, memberikan verifikasi visual bahwa pin GPIO 18 pada Raspberry Pi belum mengirimkan sinyal digital ke modul relay sehingga kunci elektrik *solenoid* tetap mengunci demi menjaga keamanan ruangan.

4.3.2.2 Tampilan Proses Pendaftaran Wajah Baru (Register *Face*)

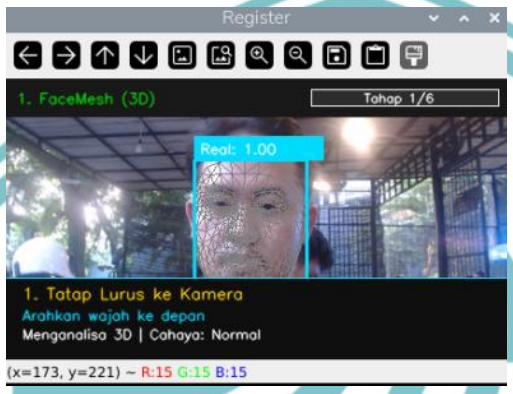
Proses pendaftaran pengguna baru dioperasikan melalui antarmuka khusus yang menerapkan pemeriksaan keaktifan berlapis (*multi-stage liveness tracking*) dari Tahap 1 hingga Tahap 8 demi membangun data *master embedding* wajah yang valid. Sistem memandu pengguna secara interaktif melalui instruksi tekstual sekuensial pada layar LCD dengan indikator batas toleransi pergerakan (*threshold*) tertentu. Visualisasi implementasi dari alur pendaftaran wajah baru tersebut dijabarkan melalui tahapan berikut ini:

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

a) Inisialisasi Deteksi Wajah

Sebelum sistem memulai pengujian pergerakan, sistem harus mengunci posisi wajah awal pengguna dalam kondisi menghadap lurus ke arah kamera. Pustaka *MediaPipe FaceMesh* akan memetakan titik-titik biometrik wajah untuk memastikan objek di depan kamera adalah struktur wajah manusia.

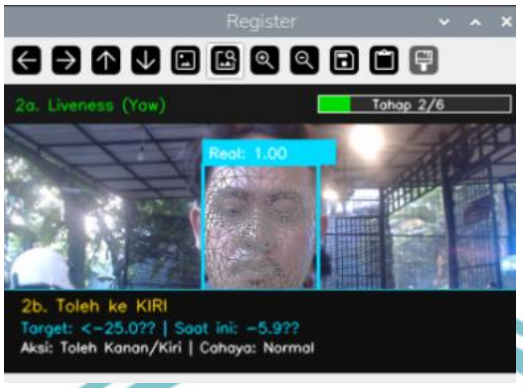


Gambar 4. 10 Deteksi Wajah Menggunakan Facemesh

Gambar 4.10 menunjukkan visualisasi tahap awal pendaftaran di mana layar monitor menampilkan kotak pembatas (*bounding box*) berwarna putih di sekeliling wajah pengguna. Pada pojok kiri atas antarmuka, muncul instruksi teks "1. Tatap Lurus ke Kamera" disertai bar informasi progres "Menahan... (x/10)". Pengguna diwajibkan mempertahankan posisi wajah di area tengah selama 10 frame konstan dengan toleransi orientasi sudut di bawah 15.0 sebelum sistem membuka gerbang tantangan berikutnya.

b) Uji Liveness Pose Acak (Randomized Pose)

Sistem registrasi menerapkan metode *randomized pose* untuk keamanan, di mana pengguna hanya diminta menyelesaikan satu jenis tantangan pose acak (geleng, angguk, atau miring kepala) setelah posisi wajah terkunci. Sebagai representasi visual antarmuka pengujian ini,



Gambar 4. 11 Pose Liveness

Meskipun Gambar 4.11 hanya menampilkan instruksi untuk toleh kiri, sistem secara utuh diprogram untuk mengevaluasi salah satu dari tiga rotasi biometrik secara acak. Jika sistem memilih pose geleng kepala (sudut *Yaw*), pengguna akan dipandu menoleh ke kanan hingga melewati batas *threshold* 25.0 selama minimal 3 *frame*, lalu ditahan lurus sebelum berlanjut menoleh ke kiri dengan *threshold* -25.0. Apabila pose angguk kepala (sudut *Pitch*) yang terpilih, layar memunculkan instruksi agar pengguna mendongak ke atas (*threshold* -20.0) lalu menunduk ke bawah (*threshold* 20.0). Sedangkan pada skenario pose miring kepala (sudut *Roll*), pengguna diwajibkan memiringkan wajah ke arah bahu kanan (*threshold* -25.0) dan ke arah bahu kiri (*threshold* 25.0) setelah posisi kepala dikembalikan menghadap depan pada setiap transisi gerakannya.

c) Uji Liveness Kedipan Mata (*Blink Eye*)

Setelah lolos dari enam pengujian gerakan kepala, sistem melakukan validasi keaktifan organ mata untuk memastikan objek bukan merupakan topeng ataupun foto wajah statis. Tahap ini diproses melalui ekstraksi nilai *Eye Aspect Ratio* (EAR) pada kelopak mata pengguna.

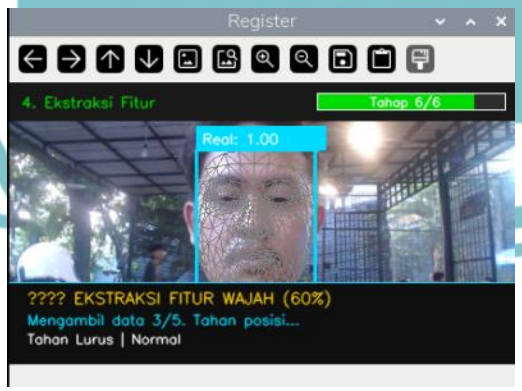
© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4. 12 Liveness Kedipan Mata (Bling Eye)

Gambar 4.12 menunjukkan jalannya proses pengujian kedipan mata pada layar alat. Sistem terlebih dahulu mewajibkan pengguna diam menatap kamera selama 15 frame guna mengalkulasi dan mengunci nilai acuan dasar kelopak mata terbuka (*base open EAR*) secara aktual sesuai kondisi intensitas cahaya ruangan. Setelah kalibrasi selesai, layar menampilkan instruksi "5. Kedipkan Mata (2x)". Sistem melacak pergerakan secara adaptif dan menghitung siklus kedipan alami berhasil terpenuhi sebanyak 2 kali ketika nilai EAR turun mencapai batas mata tertutup lalu membuka kembali.

d) Ekstraksi Fitur Biometrik

Ketika seluruh rangkaian dari Tahap 0 hingga Tahap 7 berhasil dilewati pengguna tanpa ada kesalahan orientasi gerakan, sistem menghentikan proses pengujian keaktifan dan beralih ke fungsi pemrosesan data biometrik.



Gambar 4. 13Ekstraksi Fitur Biometrik

Gambar 4.13 menampilkan kondisi final dari pendaftaran wajah baru di mana pengguna telah sukses melewati seluruh parameter tantangan *liveness*. Layar LCD memunculkan indikator teks berwarna hijau berupa pesan "Semua Liveness

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

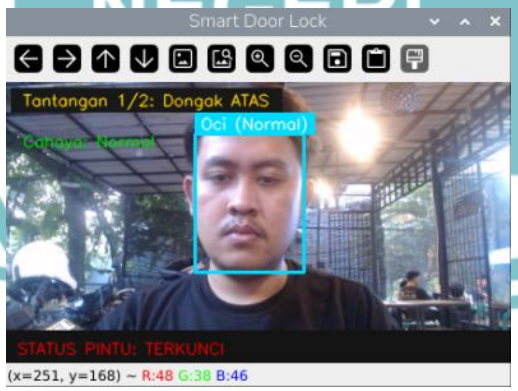
Berhasil!" disertai keterangan tindakan "Mengekstrak MobileFaceNet..." di pojok kiri atas antarmuka. Pada tahapan ini, sistem mengambil cuplikan gambar wajah dengan kualitas terbaik, mengekstraksi karakteristik uniknya menjadi kode matriks numerik (*embedding vector*), menggenerasikan ID pengguna baru, lalu menyimpan seluruh informasi tersebut ke dalam database.

4.3.2.3 Tampilan Face Recognition (Proses Pengenalan Identitas)

Begitu posisi wajah terkunci, sistem secara paralel mengeksekusi fungsi pengenalan wajah (*face recognition*) untuk memverifikasi karakteristik biometrik pengguna dengan data *master embedding* pada database. Gambar wajah di dalam kotak pembatas (*bounding box*) akan dipotong (*crop*) dan diekstraksi oleh model *MobileFaceNet* menjadi larik numerik. Guna menjaga akurasi pencocokan dari risiko degradasi visual, sistem secara adaptif menerapkan teknik peningkatan citra CLAHE (*Contrast Limited Adaptive Histogram Equalization*) dan pemetaan iluminasi (*mapping illumination*) sesuai kondisi pencahayaan ruangan yang terdeteksi.

a) Pencocokan Wajah pada Kondisi Cahaya Normal

Kondisi pencahayaan normal (*normal light*) merupakan situasi ideal di mana sebaran cahaya buatan maupun alami menyinari area wajah pengguna secara merata tanpa memicu munculnya bayangan ekstrem atau intensitas yang berlebih.



Gambar 4. 14Pencocokan Wajah Kondisi Normal

Gambar 4.14 menunjukkan visualisasi antarmuka sistem saat melangsungkan proses pengenalan wajah pada kondisi cahaya normal. Pada layar monitor LCD, sistem mengunci struktur wajah dengan kotak pembatas (*bounding box*) berwarna putih. Batas ambang kemiripan (*match threshold*) pada situasi ini mengacu pada

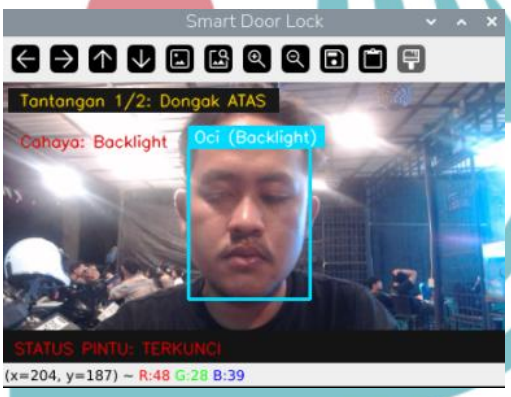
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

nilai dasar konfigurasi sistem, yaitu sebesar 0.70. Jika hasil kalkulasi matematis *Cosine Similarity* antara wajah aktual dan database memenuhi parameter tersebut, sistem akan mengidentifikasi nama pengguna dan segera mengalihkan proses menuju tahap uji keaktifan fisis (*liveness challenge*).

b) Pencocokan Wajah pada Kondisi Cahaya *Backlight*

Kondisi cahaya latar (*backlight*) terjadi ketika sumber pencahayaan di belakang objek jauh lebih kuat ketimbang cahaya yang menerpa wajah pengguna, sehingga memicu efek siluet yang membuat guratan fitur biometrik wajah tampak cenderung gelap.



Gambar 4. 15Pencocokan Wajah Kondisi Cahaya Backlight

Gambar 4.15 mengilustrasikan visualisasi antarmuka proses pengenalan wajah di bawah pengaruh efek *backlight*. Demi memulihkan detail tekstur wajah yang samar, perangkat lunak mengaktifkan fungsi penyesuaian kecerahan melalui teknik *mapping illumination*. Selain itu, sistem secara otomatis menurunkan ambang batas kecocokan (*match threshold*) sebesar -0.05 dari nilai dasar (menjadi 0.65). Mekanisme kompensasi ini menjaga sistem agar tetap sensitif dan andal dalam mengenali identitas pengguna meski dihadapkan pada tantangan pencahayaan yang kurang mendukung.

c) Pencocokan Wajah pada Kondisi Cahaya *Low Light*

Kondisi cahaya redup (*low light*) terdeteksi apabila ruangan di sekitar perangkat kekurangan pasokan cahaya, yang ditandai dengan penurunan nilai rata-rata tingkat kecerahan (*grayscale*) pada area wajah hingga di bawah batas minimum.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4. 16Pencocokan Wajah pada Kondisi Cahaya Low Light

Gambar 4.16 menunjukkan respons sistem ketika dihadapkan pada lingkungan yang gelap atau kekurangan cahaya. Pada pengkondisian lingkungan yang redup ini, sistem secara otomatis meningkatkan batas kliping (*clip limit*) CLAHE menjadi 2.0 guna mempertegas kembali tepian struktur wajah yang kabur akibat kegelapan. Guna mengantisipasi kegagalan verifikasi akibat degradasi kualitas citra, toleransi kecocokan disesuaikan dengan menurunkan *match threshold* secara otomatis sebesar -0.03 dari nilai dasar sehingga menjadi 0.67. Optimalisasi dinamis ini terbukti efektif menekan angka penolakan palsu (*False Rejection Rate*) sehingga model ekstraksi fitur *MobileFaceNet* tetap dapat bekerja optimal dalam mengenali pengguna tanpa mengorbankan integritas keamanan sistem.

4.3.2.4 Tampilan Proses Liveness Detection (Challenge-Response Autentikasi)

Setelah identitas wajah pengguna berhasil dikenali oleh sistem, perangkat tidak langsung membuka pintu, melainkan mengalihkan proses ke tahap pengujian keaktifan (*liveness detection*). Proses autentikasi interaktif ini mewajibkan pengguna menyelesaikan dua tahapan verifikasi keaktifan fisis, yaitu satu gerakan tantangan posisi kepala acak dan diikuti oleh tantangan kedipan mata. Pengondisian ini dipantau secara ketat menggunakan parameter batas *threshold* numerik konstan untuk memastikan bahwa objek di depan kamera adalah manusia hidup, bukan sebuah media statis atau replika palsu.

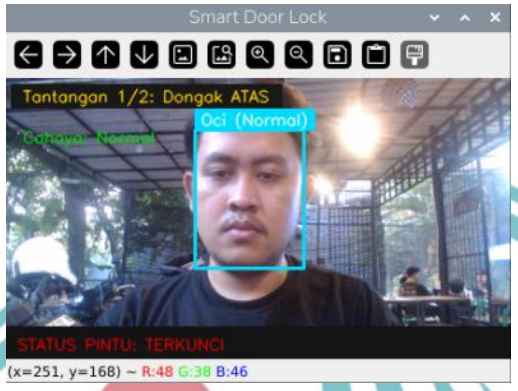
a) Uji Liveness Pose Kepala Acak (*Pose Random*)

Langkah pertama dari uji keaktifan wajah dilakukan dengan memberikan perintah pergerakan kepala yang dipilih secara acak oleh sistem dari kamus tantangan (*head*

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

pose estimation). Langkah ini bertujuan untuk memvalidasi interaksi dimensi 3D dari struktur fisis kepala pengguna secara dinamis.

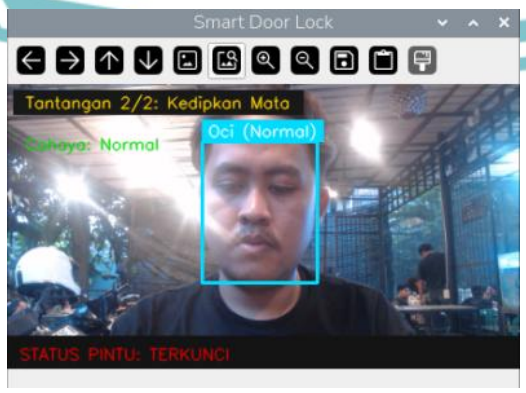


Gambar 4. 17 Liveness Pose Kepala Acak

Gambar 4.17 menunjukkan visualisasi saat sistem mengacak perintah pergerakan kepala secara *real-time*. Pada layar monitor LCD, sistem mengunci area wajah pengguna dengan kotak pembatas (*bounding box*) berwarna putih. Di pojok kiri atas antarmuka, sistem menampilkan identitas sementara pengguna berupa nama akun terdaftar beserta teks instruksi tantangan acak, contohnya "Tantangan 1/2: Toleh KANAN". Pengguna diwajibkan melakukan rotasi kepala ke arah kanan hingga nilai kalkulasi orientasi sudut *Yaw* berhasil melewati batas parameter *threshold* konstan 25.0 agar dapat dinyatakan lolos menuju tantangan kedua.

b) Uji Liveness Kedipan Mata (*Blink Eye*)

Setelah pengguna berhasil menyelesaikan tantangan pergerakan kepala acak, sistem langsung mengalihkan pengujian menuju parameter keaktifan organ mata. Langkah kedua ini berfungsi sebagai proteksi tambahan untuk mendeteksi refleks alami kelopak mata manusia.



Gambar 4. 18 Liveness Kedipan Mata (Blink Eye)

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

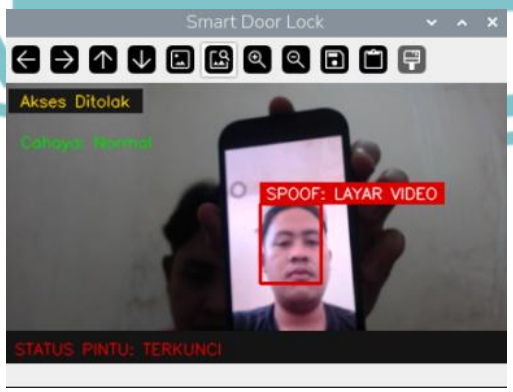
Gambar 4.18 mengilustrasikan visualisasi langkah kedua setelah pengguna berhasil menyelesaikan tantangan pergerakan kepala. Di pojok kiri atas monitor LCD, indikator perintah secara otomatis berubah menjadi teks tuntunan "Tantangan 2/2: Kedipkan Mata". Pada tahapan ini, sistem secara adaptif mengevaluasi nilai persentase kelopak mata menggunakan formula *Eye Aspect Ratio* (EAR). Siklus kedipan mata pengguna dinyatakan berhasil terekam apabila nilai EAR kelopak mata terdeteksi turun mencapai batas *threshold* konstan 0.21 lalu membuka kembali secara alami.

4.3.2.5 Tampilan Deteksi Spoofing (Anti-Spoofing)

Untuk menjaga integritas dan keamanan hak akses, sistem dilengkapi dengan modul deteksi keaktifan (*anti-spoofing*) hibrida yang bekerja secara otomatis sebelum pintu terbuka. Modul ini bertugas menganalisis tekstur citra, pantulan cahaya, dan kedalaman visual guna membedakan antara wajah asli manusia (*bona fide*) dengan upaya manipulasi menggunakan media tiruan. Sistem dikondisikan untuk mampu mengenali dan menghadang berbagai variasi serangan pemalsuan, baik serangan berbasis digital maupun cetak.

a) Deteksi Serangan Berbasis Media Layar Digital (*Layar Video*)

Serangan jenis ini memanfaatkan perangkat elektronik sekunder, seperti layar ponsel cerdas atau tablet, untuk menampilkan citra atau rekaman video wajah pengguna terdaftar di depan kamera sistem guna mengelabui autentikasi. Berikut adalah tampilan antarmuka ketika sistem berhasil mengidentifikasi dan memblokir jenis serangan pemalsuan digital tersebut.



Gambar 4. 19 Deteksi Serangan Layar Video

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.19 mengilustrasikan respons visual antarmuka sistem saat mendeteksi upaya manipulasi menggunakan layar gawai di bawah kondisi pencahayaan yang stabil. Begitu objek wajah buatan tertangkap oleh sensor kamera, algoritma *anti-spoofing* secara instan mengunci area tersebut dengan kotak pembatas (*bounding box*) berwarna merah dan menampilkan label peringatan tegas "SPOOF: LAYAR VIDEO".

Meskipun pengujian dilakukan pada lingkungan dengan indikator "Cahaya: Normal", sistem secara cerdas mampu mengenali ketidakaslian tekstur citra dari layar digital tersebut. Sebagai tindakan pengamanan otomatis, status hak akses pada sudut kiri atas langsung berubah menjadi "Akses Ditolak", sementara pergerakan komponen motor pengunci elektrik tetap ditahan dengan menampilkan konfirmasi teks berwarna merah di baris bawah, yaitu "STATUS PINTU: TERKUNCI".

b) Deteksi Serangan Berbasis Media Cetak (*Foto Cetak*)

Serangan pemalsuan menggunakan media cetak (*print attack*) dilakukan dengan cara mengarahkan lembaran foto fisik cetak dua dimensi dari wajah pengguna sah ke arah sensor kamera. Berikut adalah tampilan antarmuka saat sistem berhasil mendeteksi dan menghadang metode pemalsuan fisik tersebut:

Gambar 4. 20 Deteksi Serangan Foto Cetak

Gambar 4.20, menunjukkan visualisasi antarmuka sistem yang berhasil menggagalkan serangan pemalsuan menggunakan dokumen foto cetak. Pengujian ini dilakukan di bawah kondisi pencahayaan ideal, sebagaimana ditunjukkan oleh indikator "Cahaya: Normal". Algoritma *anti-spoofing* tetap bekerja secara andal dengan mendeteksi wajah pada foto cetak dan menandainya menggunakan kotak pembatas merah disertai teks peringatan "SPOOF: FOTO CETAK" serta

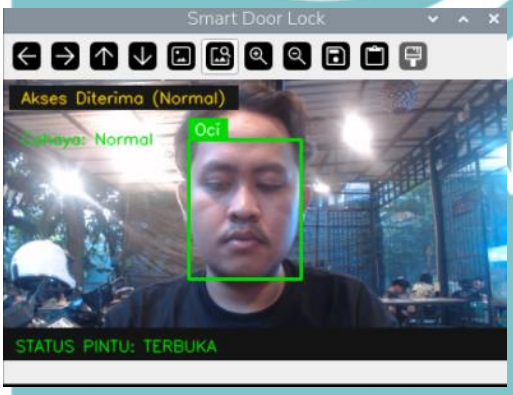
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

memunculkan status "Akses Ditolak". Karena objek terbukti tidak memiliki karakteristik keaktifan fisis manusia hidup (*liveness detection*), logika program secara otomatis menahan pergerakan pengunci elektronik dan mempertahankan pesan indikator "STATUS PINTU: TERKUNCI" guna mencegah terjadinya pembobolan akses ruangan.

4.3.2.6 Tampilan Akses Berhasil

Ketika wajah pengguna berhasil diidentifikasi cocok dengan data *master embedding*, sistem langsung mengalihkan proses ke tahap pengujian keaktifan (*liveness detection*). Setelah seluruh tantangan gerakan acak dan kedipan mata sukses diselesaikan, status validasi otomatis berubah menjadi mode terbuka (*unlocked*). Pada tahapan final ini, perangkat lunak memberikan hak akses penuh dengan mengirimkan instruksi digital menuju komponen perangkat keras. Seluruh transisi data dan respon visual pada layar monitor LCD dirancang untuk memberikan konfirmasi instan kepada pengguna bahwa autentikasi telah dinyatakan sah.



Gambar 4. 21Tampilan Akses Berhasil

Gambar 4.21 menunjukkan visualisasi antarmuka layar monitor LCD ketika pengguna berhasil mendapatkan hak akses masuk. Sistem secara otomatis mengubah warna kotak pembatas (*bounding box*) di sekeliling wajah pengguna menjadi warna hijau setelah mendeteksi kecocokan identitas biometrik dan keberhasilan uji keaktifan wajah. Pada pojok kiri atas layar, sistem menampilkan teks nama pengguna yang dikenali beserta informasi kondisi pencahayaan aktual, contohnya "Fahrul Rosi (Normal)". Tepat di bawah nama pengguna, indikator tindakan memunculkan pesan konfirmasi "Akses Diterima (Normal)". Secara

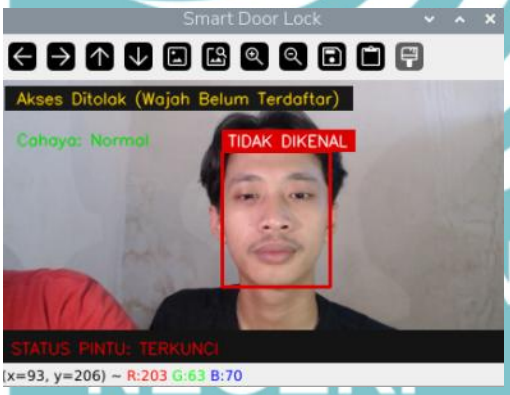
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

bersamaan, bilah bar hitam di sisi paling bawah layar berubah warna menjadi hijau dengan tulisan "STATUS PINTU: TERBUKA". Perubahan visual ini menandakan bahwa pin GPIO 18 pada Raspberry Pi telah berhasil mengirimkan sinyal digital ke modul relay untuk mengaktifkan kunci elektrik *solenoid* selama 5 detik hingga pintu dapat terbuka secara fisik.

4.3.2.7 Tampilan Akses Ditolak

Sistem *smart door lock* ini dikonfigurasikan untuk menolak seluruh upaya pembukaan kunci pintu oleh individu yang karakteristik fitur biometrik wajahnya belum teregistrasi di dalam repositori basis data. Mekanisme penolakan ini merupakan perimeter keamanan utama untuk mencegah masuknya pihak asing (*unauthorized personnel*) ke dalam ruangan yang dilindungi. Berikut adalah tampilan visual antarmuka sistem saat mendeteksi dan mengidentifikasi wajah asing yang tidak terdaftar:



Gambar 4. 22 Tampilan Akses Ditolak

Gambar 4.22 menunjukkan respons antarmuka grafis sistem ketika sensor kamera menangkap objek wajah yang datanya tidak cocok dengan seluruh data master pengguna terdaftar. Saat proses pemindaian dan ekstraksi fitur selesai dilakukan, program secara otomatis menandai area wajah subjek dengan kotak pembatas (*bounding box*) berwarna merah disertai label penanda teks "TIDAK DIKENAL" tepat di atasnya.

Meskipun kondisi pencahayaan di sekitar ruangan terdeteksi ideal pada indikator "Cahaya: Normal", sistem tetap menolak hak akses secara mutlak. Hal ini dibuktikan dengan munculnya bilah notifikasi peringatan berwarna kuning di sudut kiri atas yang menegaskan pesan "Akses Ditolak (Wajah Belum Terdaftar)". Secara

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

simultan, logika pemrograman internal menahan pergerakan komponen motor pengunci elektrik dan menampilkan status konfirmasi akhir pada baris bawah antarmuka dengan teks "STATUS PINTU: TERKUNCI".

4.3.3 Implementasi Basis Data

Implementasi basis data pada sistem *smart door lock* ini menerapkan pendekatan penyimpanan ganda (*hybrid storage*) dengan mengintegrasikan SQLite lokal pada Raspberry Pi untuk kebutuhan verifikasi luring (*offline*) secara lancar, serta Supabase Cloud (PostgreSQL) sebagai cadangan data terpusat di server awan. Proses sinkronisasi data antar-kedua platform dikendalikan secara otomatis dan asinkron oleh utas latar belakang (*background sync worker thread*) setiap kali terjadi transaksi data baru. Guna memaksimalkan efisiensi operasi I/O pada perangkat keras berspesifikasi terbatas, koneksi SQLite dioptimalkan melalui pengaktifan mode jurnal berbasis memori (*memory journal mode*) dan tingkat sinkronisasi normal. Selain itu, untuk menjaga konsistensi skema relasional, sistem menerapkan aturan *Foreign Key constraint* serta mekanisme *Database Triggers*, di mana setiap penghapusan data secara lokal akan otomatis mencatat ID rekaman ke dalam tabel penampung sync_deletes agar server Supabase dapat melakukan penghapusan data secara simetris dari jarak jauh.

Sebagai bentuk penguatan keamanan data, khususnya untuk melindungi data biometrik yang bersifat sensitif, sistem menerapkan mekanisme enkripsi pada data fitur wajah (*embedding*) hasil ekstraksi model *MobileFaceNet* sebelum disimpan ke dalam basis data. Proses enkripsi ini menggunakan algoritma *Advanced Encryption Standard* 256-bit (AES-256) yang diimplementasikan melalui pustaka (*library*) *PyCryptodome* pada bahasa pemrograman Python. Data *embedding* wajah ini dienkripsi secara konsisten pada kedua sisi penyimpanan, baik pada basis data lokal SQLite di perangkat Raspberry Pi maupun pada basis data *cloud* Supabase (PostgreSQL), sehingga apabila terjadi kebocoran atau akses tidak sah terhadap berkas basis data, data biometrik pengguna tetap terlindungi dan tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Adapun data non-biometrik lainnya, seperti nama pengguna dan *log* riwayat akses, tetap disimpan dalam bentuk teks biasa karena tidak bersifat sensitif secara biometrik.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

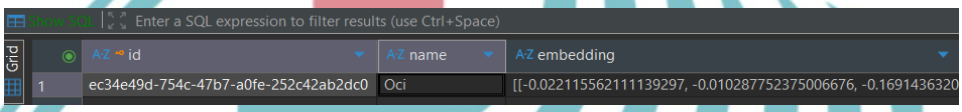
Output data aktual yang berhasil diimplementasikan ke dalam sistem arsitektur basis data ini terbagi ke dalam tiga tabel utama, yaitu sebagai berikut:

4.3.3.1 Tabel Wajah Pengguna (registered_faces)

Tabel ini mengelola informasi identitas utama pengguna terdaftar yang menampung karakteristik unik wajah hasil ekstraksi model *MobileFaceNet* beserta parameter ambang batas gerakan.

a) Basis Data Lokal (SQLite)

Berikut adalah tampilan data master wajah pendaftar yang berhasil disimpan ke dalam media penyimpanan lokal perangkat:

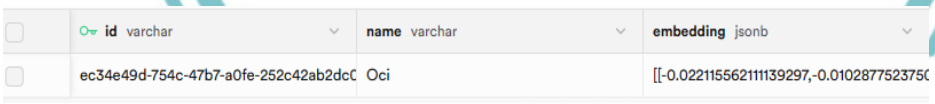


Gambar 4. 23Basis Data Lokal Wajah Pengguna

Gambar 4.23 menunjukkan data master pengguna terdaftar yang tersimpan pada penyimpanan lokal SQLite. Berdasarkan tampilan tersebut, kolom id menampung nilai UUID unik berupa teks identifikasi registrasi acak untuk mencegah duplikasi data, kolom name menyimpan nama pengguna murni, serta kolom embedding berisi kumpulan data larik matriks fitur biometrik wajah terkompresi. Kolom liveness_config menampung konfigurasi parameter keaktifan wajah untuk mendukung proses validasi interaktif.

b) *Cloud* Database (Supabase)

Berikut adalah visualisasi hasil sinkronisasi data master wajah pengguna yang berhasil diunggah ke server awan terpusat:



Gambar 4. 24 Basis Data Supabase Wajah Pengguna

Gambar 4.24 menunjukkan data master wajah yang sukses tersinkronisasi pada dasbor tabel Supabase Cloud. Keselarasan tipe data pada server awan diwujudkan dengan mendefinisikan kolom id dan name sebagai string berkapasitas dinamis (VARCHAR(255)). Sementara itu, kolom embedding dan liveness_config dikonfigurasikan secara khusus menggunakan tipe data JSONB (*Binary JSON*)

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

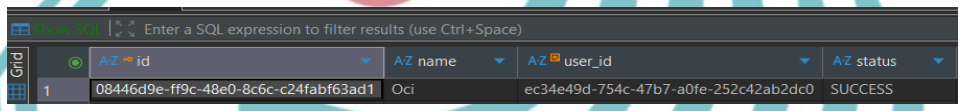
untuk mengoptimalkan efisiensi penyimpanan objek array kompleks. Nilai latensi dipetakan ke dalam format pecahan FLOAT8, diikuti dengan pencatatan waktu otomatis berbasis zona waktu global (TIMESTAMPTZ).

4.3.3.2 Tabel Log Registrasi Wajah (register_logs)

Tabel ini berfungsi sebagai rekam jejak digital untuk mendokumentasikan status akhir serta keberhasilan proses pemenuhan tantangan gerakan kepala dan mata saat pendaftaran pengguna baru dilakukan.

a) Basis Data Lokal (SQLite)

Berikut adalah tampilan log hasil pencatatan riwayat pendaftaran wajah baru pengguna pada sistem penyimpanan lokal alat:

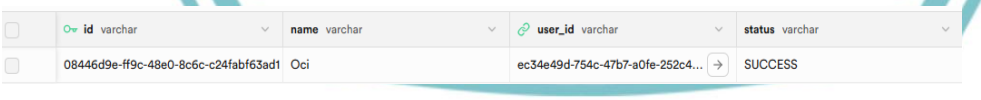


Gambar 4. 25Basis Data Lokal Log Registrasi

Gambar 4.25 menampilkan log transaksi pendaftaran wajah pada SQLite lokal. Baris data tersebut memperlihatkan kolom id sebagai kode transaksi registrasi unik dan kolom name berisi nama pendaftar. Kolom user_id bertindak sebagai *foreign key* relasional dengan aturan ketergantungan ON DELETE CASCADE yang mengikat data ke tabel master wajah, sedangkan kolom status mendokumentasikan konfirmasi akhir pendaftaran dengan nilai "SUCCESS".

b) *Cloud* Database (Supabase)

Berikut adalah rekam jejak jurnal transaksi registrasi wajah pengguna yang telah berhasil dicadangkan ke dalam platform basis data *cloud*:



Gambar 4. 26 Basis Data Supabase Log Registrasi

Gambar 4.26 memperlihatkan luaran log transaksi registrasi wajah yang telah berhasil terunggah ke dasbor platform Supabase Cloud. Sesuai skema fisik eksternal, tabel ini mengimplementasikan kolom identitas string seperti id, name, dan user_id ke dalam format VARCHAR(255) dengan relasi terikat ON DELETE CASCADE. Status transaksi dikunci dalam batas karakter tertentu

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

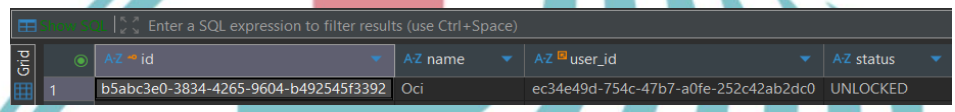
(VARCHAR(50)), sementara rekam performa fisik seperti yaw_data, pitch_data, roll_data, dan blink_data ditampung secara utuh oleh tipe data struktural teks panjang (TEXT).

4.3.3.3 Tabel Riwayat Akses Pintu (access_logs)

Tabel ini bertindak sebagai jurnal elektronik harian untuk mencatat setiap aktivitas upaya verifikasi wajah dan status akhir pembukaan kunci pada pintu ruangan.

a) Basis Data Lokal (SQLite)

Berikut adalah visualisasi rekaman riwayat log harian akses keluar masuk pintu yang tercatat pada penyimpanan internal:

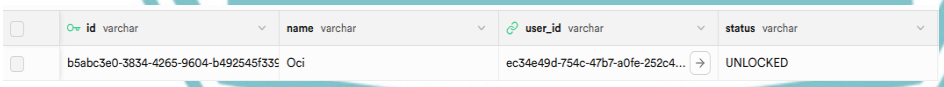


Gambar 4. 27 Basis Data Lokal Akses Pintu

Gambar 4.27 mengilustrasikan baris riwayat transaksi akses pada SQLite lokal. Berdasarkan luaran tersebut, kolom id menampung nilai UUID transaksi akses dan kolom name mencatat identitas nama pengguna yang melakukan pemindaian. Kolom user_id terikat dengan kunci relasional tabel induk wajah melalui aturan integritas ON DELETE SET NULL, serta status pembukaan kunci elektrik pintu terekam secara valid pada kolom status dengan nilai "UNLOCKED".

b) *Cloud* Database (Supabase)

Berikut adalah log riwayat akses autentikasi pintu pengguna yang berhasil terkirim dan tercatat di dalam dasbor monitoring:



Gambar 4. 28 Basis Data Supabase Akses Pintu

Gambar 4.28 menunjukkan visualisasi data log akses pintu yang sama namun telah berhasil dikirimkan ke server Supabase Cloud secara *real-time*. Pada arsitektur awan ini, kolom user_id diselaraskan sebagai VARCHAR(255) untuk menjaga validitas relasi eksternal dengan aturan ON DELETE SET NULL. Kolom pengukur akurasi model (accuracy) serta rincian waktu komputasi fisis (face_val_latency_ms

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

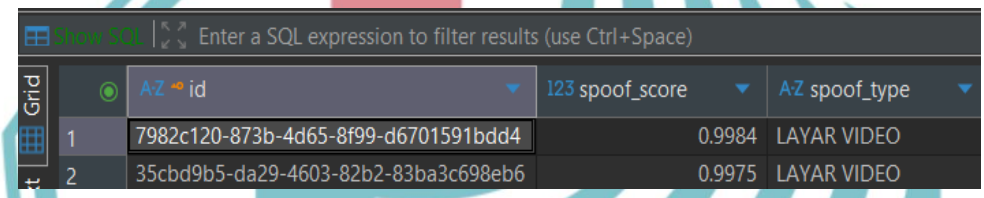
dan auth_latency_ms) didefinisikan menggunakan format numerik presisi tinggi (FLOAT8) guna menyediakan akurasi metrik desimal yang valid.

4.3.3.4 Tabel Log Serangan (spoofing_logs)

Tabel ini dirancang khusus untuk mendata setiap upaya manipulasi atau serangan pemalsuan wajah (*spoofing attack*) yang berhasil dideteksi dan digagalkan oleh sistem.

a) Basis Data Lokal (SQLite)

Berikut adalah jurnal pencatatan indikasi serangan manipulasi wajah ilegal yang berhasil dihadang oleh sistem secara lokal pada database:

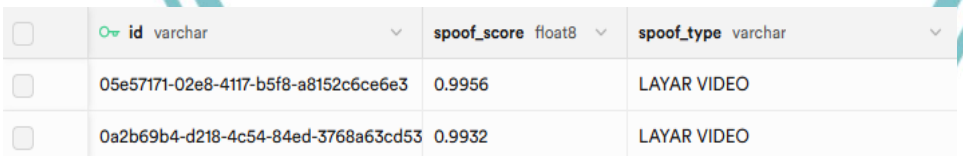


Gambar 4. 29 Basis Data Lokal Log Serangan

Gambar 4.29 menunjukkan visualisasi luaran data serangan palsu yang terekam pada SQLite lokal. Perangkat mendokumentasikan nilai presisi tingkat kecurigaan serangan pada kolom spoof_score yang mendekati nilai ideal maksimal, serta mengklasifikasikan jenis kategori media peretasan ilegal yang teridentifikasi oleh algoritma pada kolom spoof_type.

b) *Cloud* Database (Supabase)

Berikut adalah visualisasi penyimpanan data log anti-spoofing yang tersinkronisasi aman pada sistem komputasi awan server:



Gambar 4. 30Basis Data Supabase Log Serangan

Gambar 4.30 menampilkan visualisasi log serangan *spoofing* yang telah tersinkronisasi pada platform Supabase Cloud. Luaran gambar ini menunjukkan implementasi fisik kolom id ke dalam batasan tipe string VARCHAR(255) dan kolom spoof_type ke dalam batasan string VARCHAR(50). Demi mempertahankan

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

tingkat kepresisian evaluasi sistem anti-pemalsuan, nilai ambang kecurigaan pada kolom spoof_score serta metrik performa spoof_latency_ms dikonfigurasikan secara presisi menggunakan format data pecahan mengambang berkapasitas 8-byte (FLOAT8).

4.4 Pengujian

Setelah perancangan prototipe *smart door lock* berbasis IoT dan pengenalan wajah selesai, tahap selanjutnya adalah pengujian menyeluruh untuk memastikan sistem beroperasi sesuai target penelitian. Pengujian ini bertujuan untuk memvalidasi integrasi perangkat keras dan lunak, menguji ketahanan keamanan dari manipulasi wajah (*anti-spoofing*), menentukan batas optimal sensor kamera, menghitung akurasi algoritma kecerdasan buatan (*MobileFaceNet*), serta mengukur kualitas transmisi data jaringan (*Quality of Service*). Agar terstruktur secara ilmiah, pemaparan pada subbab ini dibagi menjadi empat bagian utama: deskripsi pengujian, prosedur pengambilan data, hasil eksperimen, dan ditutup dengan analisis serta evaluasi performa sistem.

4.4.1 Deskripsi Pengujian

Menjelaskan batasan dan tujuan dari pengujian alat pengunci pintu pintar (*smart door lock*) berbasis pengenalan wajah dan *Internet of Things* (IoT) untuk mengukur seberapa baik sistem ini bekerja secara nyata. Agar penilaian berjalan rapi, jujur, dan adil, seluruh rangkaian percobaan dibagi ke dalam delapan tahapan uji coba yang berjalan berurutan, yaitu pengujian fungsi dasar alat (*blackbox testing*), pengujian ketahanan mesin Raspberry Pi (mengecek suhu dan penggunaan RAM), serta pengujian keamanan *liveness* untuk memastikan sistem tidak bisa dibohongi oleh foto cetak atau rekaman video di HP. Selanjutnya, dilakukan pengujian untuk mencari jarak berdiri paling pas di depan kamera, pengujian ketahanan sistem saat pengguna memakai aksesoris (seperti kacamata, topi, masker) atau saat kondisi lampu ruangan berubah, pengujian kecepatan waktu respons alat, pengujian akurasi cerdas model *MobileFaceNet* lewat perhitungan *Confusion Matrix* (mencari nilai *Accuracy, Precision, Recall,* dan *F1-Score* pada kondisi terbaik), hingga ditutup dengan pengujian kualitas transmisi jaringan (*Quality of Service*) untuk melihat kecepatan pengiriman log data akses. Seluruh proses pengambilan data ini dilakukan langsung pada perangkat keras lokal Raspberry Pi 4 Model B yang

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

dipasangkan dengan modul kamera, *relay*, dan kunci elektrik *solenoid*, sementara bagian programnya mengombinasikan deteksi titik wajah *MediaPipe*, kecerdasan buatan *MobileFaceNet* (ONNX), serta sistem pengiriman data IoT secara *real-time*.

4.4.2 Prosedur Pengujian

Prosedur Pengujian disusun sebagai panduan eksperimen terstruktur yang diawali dengan pengujian fungsionalitas metode *black-box* untuk memvalidasi sembilan skenario fitur utama sistem. Langkah berikutnya adalah pengujian stabilitas komputasi perangkat keras lewat perekaman data untuk mengukur secara presisi rata-rata durasi waktu dan beban utilitas CPU aplikasi dari awal hingga selesai proses pada Mode Registrasi pengguna baru, serta performa CPU *main* dan durasi pemrosesan pada Mode Verifikasi wajah dari saat wajah pertama kali terdeteksi hingga pin GPIO aktif memicu relai untuk membuka kunci *solenoid door lock*. Selanjutnya, pengujian keandalan gerbang *anti-spoofing* dilakukan melalui 10 kali repetisi paparan wajah asli, foto cetak, dan layar video digital. Alur eksperimen diteruskan dengan analisis pengaruh variasi jarak fisik tegak lurus (40 cm, 60 cm, 80 cm, dan 100 cm) terhadap nilai *Cosine Score* , diikuti pengujian ketahanan ekstraksi fitur terhadap halangan aksesoris wajah (topi, kacamata, masker) serta fluktuasi intensitas cahaya ekstrem (*low-light* dan *backlight*). Seluruh rangkaian prosedur ini ditutup dengan pengambilan 100 sampel acak dari kelompok wajah terdaftar dan asing untuk dipetakan ke dalam *Confusion Matrix* guna mengevaluasi persentase akhir dari metrik akurasi, presisi, sensitivitas, dan *F1-Score*.

4.4.3 Data Hasil Pengujian

Bagian ini menyajikan seluruh data mentah yang diperoleh secara nyata dari rangkaian eksperimen yang telah dilakukan sesuai dengan prosedur pada subbab sebelumnya. Seluruh data rekaman hasil pengujian, mulai dari fungsi dasar alat, ketahanan fisik komputer Raspberry Pi, hasil deteksi sistem keamanan *liveness*, pengaruh jarak dan cahaya, kecepatan waktu respons, pemetaan akurasi kecerdasan model, hingga kualitas pengiriman data jaringan dituangkan secara jujur dan objektif ke dalam bentuk tabel-tabel berikut.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.4.3.1 Pengujian Fungsionalitas

Pengujian fungsionalitas dilakukan untuk memastikan bahwa seluruh fitur dan komponen mekanis pada sistem *smart door lock* berbasis *Internet of Things* berjalan dengan benar. Metode yang digunakan adalah *black-box testing*, yaitu pengujian yang berfokus pada fungsi masukan dan luaran sistem tanpa menganalisis detail kode program di dalamnya.

Melalui pengujian ini, setiap elemen seperti penangkapan gambar oleh kamera, pemrosesan wajah, tampilan instruksi pada layar LCD, hingga respons kunci pintu elektrik dievaluasi. Tujuannya adalah untuk memastikan seluruh sistem bekerja stabil dan sesuai dengan rancangan keamanan yang telah ditetapkan. Data hasil pengujian fungsionalitas disajikan secara ringkas dalam Tabel 4.12.

Tabel 4.12 Pengujian Fungsional

No	Fitur / Komponen yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Status
1	Inisialisasi Sistem dan Kamera	Perangkat dinyalakan dan program utama dijalankan dari kondisi awal.	Layar LCD menampilkan video kamera secara lancar, muncul status "Mencari Wajah...", dan kunci pintu dalam kondisi terkunci rapat.	Sesuai
2	Mode Pendaftaran (*Register Mode*)	Admin memasukkan identitas baru untuk merekam wajah pengguna baru.	Kamera aktif menangkap gambar wajah, sistem berhasil memetakan titik geometri wajah, dan layar	Sesuai

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Fitur / Komponen yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Status
			menampilkan panduan registrasi.	
3	Validasi *Liveness* Saat Registrasi	Pengguna melakukan gerakan kepala dan kedipan mata sesuai instruksi sistem saat mendaftar.	Sistem mendeteksi pergerakan wajah secara akurat, mengekstrak data karakteristik biometrik, lalu menyimpannya ke database lokal.	Sesuai
4	Autentikasi Pengguna Sah (*Access Granted*)	Pengguna yang sudah terdaftar berdiri di depan kamera.	Wajah dikenali dengan skor kecocokan yang sesuai, tantangan keaktifan wajah tervalidasi, layar memunculkan pesan "Akses Diterima", dan bar status berubah hijau.	Sesuai
5	Pengendalian Kunci Elektrik	Autentikasi wajah dinyatakan sah dan lolos dari uji keaktifan fisis.	Mikrokontroler mengirim sinyal untuk memicu relay, kunci	Sesuai

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Fitur / Komponen yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Status
			solenoid terbuka secara otomatis, dan pintu dapat dibuka selama 5 detik.	
6	Identifikasi Pengguna Asing (*Access Denied*)	Orang yang wajahnya belum terdaftar berdiri dan memindai wajah di depan kamera.	Kotak pembatas wajah di layar berwarna merah dengan label "TIDAK DIKENAL", sistem menolak hak akses, dan pintu tetap terkunci. memproses citra wajah.	Sesuai
7	Tombol Keluar Manual (*Push Button*)	Pengguna menekan tombol saklar fisik yang terpasang di dalam ruangan.	sistem mendeteksi input tombol, relay langsung terpicu, dan kunci solenoid terbuka seketika tanpa perlu memproses citra wajah.	Sesuai
8	Mekanisme *State Machine Reset*	Pengguna menjauh atau menghilang dari	Sistem mendeteksi hilangnya wajah,	Sesuai

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Fitur / Komponen yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Status
		jangkauan kamera saat tantangan keaktifan sedang berlangsung.	otomatis membatalkan tahapan verifikasi yang sedang berjalan, dan kembali ke kondisi siaga awal.	
9	Jurnal Akses dan Sinkronisasi	Proses verifikasi wajah selesai dilakukan (akses berhasil, ditolak, atau deteksi manipulasi wajah).	Riwayat aktivitas terekam ke database lokal dan langsung terkirim ke database cloud melalui internet tanpa membuat tampilan layar menjadi lambat.	Sesuai

Berdasarkan data hasil pengujian pada Tabel 4.12, dapat disimpulkan bahwa seluruh fitur utama dan komponen pendukung pada sistem pintu pintar ini berfungsi dengan tingkat keberhasilan 100%. Integrasi antara perangkat keras dan perangkat lunak mampu bekerja secara optimal dalam menjalankan setiap skenario operasional yang diujikan.

Logika program yang dirancang terbukti andal, khususnya pada fitur pembatalan otomatis ketika wajah pengguna tiba-tiba hilang di tengah proses verifikasi. Fitur ini sangat penting untuk mencegah celah keamanan jika pengguna meninggalkan pintu sebelum proses autentikasi selesai sepenuhnya. Selain itu, tombol keluar manual dan sistem sinkronisasi data ganda (*hybrid storage*) ke server lokal maupun

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

cloud juga berjalan lancar tanpa mengganggu jalannya video streaming utama. Secara keseluruhan, hasil pengujian ini menunjukkan bahwa sistem pintu pintar telah siap dan layak diimplementasikan pada lingkungan hunian modern.

4.4.3.2 Pengujian Stabilitas Komputasi *Hardware*

Pengujian stabilitas komputasi perangkat keras dilakukan untuk mengevaluasi konsistensi, keandalan, serta reliabilitas performa *Single Board Computer* (SBC) Raspberry Pi 4 Model B ketika mengeksekusi arsitektur kecerdasan buatan secara lokal (*edge computing*). Evaluasi ini dibagi menjadi dua skenario pengujian utama, yaitu pengujian pada Mode Registrasi (*Register Mode*) dan Mode Verifikasi (*Check-in Mode*). Data aktual yang disajikan di bawah ini diambil langsung secara empiris dari rekaman log telemetri sistem dengan interval pencatatan setiap 0,5 detik melalui pustaka monitoring bawaan pada perangkat keras berspesifikasi RAM 8GB dengan arsitektur sistem operasi 64-bit.

a) Performa Pada Mode *Register*

Mode Registrasi merupakan fase komputasi dengan beban kerja paling intensif di dalam sistem karena memaksa perangkat keras menjalankan pemrosesan citra dari kamera secara terus-menerus (*looping* bertumpuk) melalui tahapan pendaftaran wajah interaktif. Data hasil pengukuran rata-rata performa perangkat keras dari 5 kali repetisi sesi pendaftaran wajah baru dirangkum pada Tabel 4.13 berikut

Tabel 4.13 Performa Pada Mode *Register*

No	Rata-rata Durasi (s)	Rata-rata CPU Proses (%)	Rata-rata CPU Sistem (%)	Rata-rata RAM Proses (MB)	Rata-rata RAM Perangkat (%)	Rata-rata Suhu CPU (°C)
1	59,22	152,1	52,3	208,35	9,5	48,9
2	41,15	178,4	62,3	234,64	9,5	48,5
3	44,59	187,3	65,2	239,50	9,6	50,0
4	43,18	178,3	63,2	235,42	9,5	52,7
5	41,14	164,2	58,2	230,65	9,7	53,7

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Rata-rata Durasi (s)	Rata-rata CPU Proses (%)	Rata-rata CPU Sistem (%)	Rata-rata RAM Proses (MB)	Rata-rata RAM Perangkat (%)	Rata-rata Suhu CPU (°C)
Rata-Rata	45,86	172,1	60,2	229,71	9,6	50,8

Berdasarkan data statistik pada Tabel 4.13, Mode Registrasi menuntut konsumsi daya CPU proses aplikasi (*proc_cpu*) yang cukup tinggi dengan rata-rata global mencapai 172,1%, di mana representasi angka di atas 100% ini sangat valid secara teoretis karena sistem operasi Linux mengakumulasikan utilitas dari setiap inti pemroses pada CPU *Quad-core* Broadcom BCM2711 Raspberry Pi 4B (bacaan maksimal sistem adalah 400%). Tingginya beban kerja ini berkolerasi langsung dengan kompleksitas pipeline algoritma hibrida yang berjalan secara simultan di setiap *frame* citra untuk memetakan topologi wajah 3D (*MediaPipe Face Mesh*) , mengalkulasikan refleks gerakan biologis (*Head Pose Estimation* dan *Eye Aspect Ratio*) , serta mengekstraksi matriks fitur biometrik (*MobileFaceNet*) sebelum disinkronkan secara asinkron ke SQLite lokal dan Supabase Cloud. Peningkatan alokasi memori RAM proses pada Mode Registrasi (rata-rata global 229,71 MB) disebabkan oleh alokasi *buffer* sementara untuk menampung variabel data *multi-stage tracking* dari awal kalibrasi gerakan keaktifan , serta pengolahan larik matriks baru hasil ekstraksi model AI sebelum ditulis ke dalam database. Kendati demikian, alokasi tersebut tetap stabil dan aman (hanya memakan sekitar 9,6% dari kapasitas RAM hardware) tanpa indikasi kebocoran memori (*memory leak*), serta menjaga kondisi suhu termal internal CPU aman dengan rata-rata global 50,8°C yang berada jauh di bawah ambang batas pelambatan kinerja fisik perangkat keras.

b) Performa Pada Mode Verifikasi

Mode Verifikasi merupakan fase operasional utama harian sirkuit prototipe untuk melayani akses masuk pengguna menggunakan gerbang tantangan interaktif acak yang lebih ringkas. Data hasil pengukuran rata-rata performa perangkat keras dari 5 kali repetisi sesi autentikasi wajah disajikan pada Tabel 4.14 berikut.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.14 Performa Pada Mode Verifikasi

No	Rata-rata Durasi (s)	Rata-rata CPU Proses (%)	Rata-rata CPU Sistem (%)	Rata-rata RAM Proses (MB)	Rata-rata RAM Perangkat (%)	Rata-rata Suhu CPU (°C)
1	13,25	34,9	48,5	210,72	9,7	48,7
2	17,29	33,7	44,7	201,63	9,5	47,8
3	16,73	33,7	44,3	199,67	9,5	48,5
4	16,26	32,5	43,0	201,45	9,5	48,2
5	16,24	32,4	42,8	199,54	9,5	48,4
Rata-Rata	15,95	**33,4**	44,7	202,60	9,5	48,3

Pada data hasil pengujian pada Tabel 4.14, implementasi sistem pada Mode Verifikasi menunjukkan tingkat efisiensi sumber daya yang jauh lebih tinggi, dicirikan oleh durasi waktu respons harian yang sangat cepat dengan rata-rata global selama 15,95 detik. Penurunan beban komputasi yang sangat drastis terlihat pada rata-rata CPU proses aplikasi yang menyusut hingga ke angka 33,4% (terpangkas sebesar 80,59% jika dibandingkan mode pendaftaran), karena pipeline sistem beralih dari fase pendaftaran kontinu ke fase inferensi tunggal (*single inference*) singkat yang hanya membutuhkan satu kali pencocokan karakteristik wajah menggunakan rumus jarak vektor *Cosine Similarity*. Efisiensi program ini berbanding lurus dengan konsumsi memori RAM proses aplikasi yang sangat stabil di kisaran rata-rata 202,60 MB (9,5% dari total kapasitas hardware) serta kondisi suhu inti prosesor yang beroperasi secara dingin di angka rata-rata global 48,3°C. Karakteristik metrik hardware yang rendah pada operasional harian ini menegaskan bahwa prototipe *smart door lock* yang dikembangkan memenuhi standar keandalan fisik (*hardware reliability*) untuk diimplementasikan secara riil secara berkelanjutan tanpa risiko panas berlebih (*overheating*).

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

c) Mitigasi Kestabilan Sistem (Thermal dan Hang/Freeze)

Sebagai langkah mitigasi terhadap risiko panas berlebih, unit Raspberry Pi 4 Model B pada prototipe ini dilengkapi dengan pendinginan aktif berupa *heatsink* dan kipas (*fan*) yang terpasang langsung pada modul *System on Chip* (SoC) perangkat. Berdasarkan hasil pengujian pada Tabel 4.13 dan Tabel 4.14, suhu CPU rata-rata tercatat stabil pada rentang 48,3°C hingga 50,8°C, jauh di bawah ambang batas *thermal throttling* Raspberry Pi 4 Model B (≈ 80°C) maupun ambang *automatic shutdown* akibat panas berlebih (≈ 85°C). Dengan demikian, kombinasi pendinginan aktif dan beban komputasi yang teroptimasi terbukti efektif mencegah penurunan performa maupun kerusakan perangkat keras akibat suhu tinggi selama pengujian berlangsung.

Di sisi lain, mitigasi terhadap potensi kegagalan perangkat lunak berupa kondisi *hang* atau *freeze* pada sistem masih menjadi keterbatasan dalam penelitian ini, karena prototipe belum dilengkapi mekanisme *watchdog timer* maupun layanan *auto-restart* otomatis. Apabila terjadi kegagalan proses aplikasi atau sistem operasi mengalami hang, pemulihan saat ini masih harus dilakukan secara manual oleh admin melalui restart perangkat. Keterbatasan ini menjadi salah satu poin rekomendasi pengembangan pada sub-bab Saran (5.2), yaitu penerapan mekanisme watchdog berbasis perangkat lunak (seperti systemd-watchdog) maupun watchdog timer perangkat keras bawaan Raspberry Pi agar pemulihan sistem dapat berjalan otomatis tanpa memerlukan intervensi manual.

d) Analisis Waktu Latensi Tahap Registrasi (*Preprocessing*)

Untuk mengetahui pada tahap mana waktu pemrosesan registrasi paling banyak terpakai, dilakukan analisis lanjutan terhadap data log mentah dari 30 sesi pendaftaran wajah yang berhasil (SUCCESS). Data ini mencatat durasi tiap komponen proses secara terpisah, mulai dari tantangan pose kepala, tantangan kedipan mata, hingga tahap pemrosesan fitur dan penyimpanan data, sebagaimana dirangkum pada Tabel 4.15 berikut.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.15 Analisis Waktu Latensi Tahap Registrasi (*Preprocessing*)

Tahap Pemrosesan	Rata-rata (ms)	Median (ms)	Minimum (ms)	Maksimum (ms)
Tantangan Pose Kepala (*Head Pose Challenge*)	650,5	437,2	203,9	4022,9
Tantangan Kedipan Mata (*Blink Challenge*)	713,8	614,4	455,0	3041,9
Pemrosesan Fitur & Penyimpanan Data (ekstraksi *FaceMesh*, *MobileFaceNet*, enkripsi, dan penyimpanan basis data)	2.632,5	2.388,9	1.817,7	8.933,5
Total Waktu Registrasi	**3.996,8**	**3.404,8**	**2.727,1**	**15.776,9**

Berdasarkan Tabel 4.15, dapat dilihat bahwa dari keseluruhan waktu registrasi, porsi waktu terbesar justru terpakai pada tahap pemrosesan fitur dan penyimpanan data (rata-rata 2.632,5 ms), bukan pada tahap interaksi pengguna seperti tantangan pose kepala (rata-rata 650,5 ms) maupun kedipan mata (rata-rata 713,8 ms). Dengan kata lain, sebagian besar waktu justru digunakan oleh sistem di balik layar untuk mengekstrak titik-titik wajah, menghitung ciri unik wajah, mengenkripsi data, dan menyimpannya ke basis data, bukan oleh kecepatan pengguna dalam mengikuti instruksi. Perlu dicatat pula bahwa dua sesi registrasi (atas nama Vira dan Fahrul Rosi) mencatat waktu jauh lebih lama dibandingkan peserta lain karena tantangan pose maupun kedipannya membutuhkan beberapa kali pengulangan sebelum berhasil, sehingga nilai median lebih tepat dijadikan acuan umum dibandingkan nilai rata-rata yang cenderung terpengaruh oleh kedua data tersebut.

4.4.3.3 Pengujian Keandalan *Liveness* & *Anti-spoofing*

Pengujian pada tahap ini dilakukan untuk mengevaluasi tingkat keandalan gerbang keamanan pertama sistem dalam membedakan karakteristik antara subjek asli (manusia hidup) dengan berbagai upaya pemalsuan (*spoofing*). Skenario pengujian dilakukan secara terpisah menggunakan sampel wajah asli serta atribut tiruan berupa foto cetak kertas dua dimensi dan rekaman video digital. Pengujian

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

dikondisikan di bawah intensitas cahaya normal ruangan untuk memetakan respon fungsional dan akurasi logika penyaringan pada sistem.

a) Skenario Spoofing Menggunakan Foto

Berikut merupakan data hasil pemantauan gerbang pertahanan biometrik ketika diuji menggunakan atribut manipulasi akses berupa media cetak foto dua dimensi:

Tabel 4.16 Skenario Spoofing Menggunakan Foto

Pengujian	Kategori Subjek	Status Liveness	Status *Liveness*	Status Pintu
1	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
2	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
3	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
4	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
5	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
6	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
7	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
8	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
9	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
10	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
11	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci

Pengujian	Kategori Subjek	Status Liveness	Status *Liveness*	Status Pintu
12	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
13	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
14	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
15	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
16	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
17	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
18	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
19	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
20	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
21	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
22	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
23	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
24	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
25	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
26	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Kategori Subjek	Status Liveness	Status *Liveness*	Status Pintu
27	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
28	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
29	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci
30	Foto Cetak	Terdeteksi Foto Cetak	Ditolak	Terkunci

Merujuk pada data hasil pengujian pada Tabel 4.16, gerbang pertahanan biometrik sistem terbukti memiliki ketahanan yang sangat tinggi terhadap upaya pemalsuan akses. Ketika dihadapkan pada media cetak kertas (2D *printed photo*), algoritma pengklasifikasi kecerdasan buatan secara instan mengenali adanya manipulasi fisik dan mengeluarkan status "Terdeteksi Foto Cetak". Karena objek visual yang dianalisis tidak memiliki kontur kedalaman spasial dan gagal memberikan respon pergerakan biologis yang riil, alur program secara otomatis memutus interaksi otentikasi. Hal ini membuat status tantangan interaksi langsung diklasifikasikan sebagai "Ditolak" tanpa memicu pemicuan langkah selanjutnya, sehingga pin kendali relai tetap berada dalam kondisi logika *LOW* atau status pintu sepenuhnya aman "Terkunci".

b) Skenario Spoofing Menggunakan Video

Skenario ketiga dilakukan untuk menguji kekuatan gerbang keamanan sistem ketika menerima manipulasi dinamis berupa rekaman video wajah pengguna asli yang diputar melalui layar *smartphone*.

Tabel 4.17 Skenario Spoofing Menggunakan Video

Pengujian	Kategori Subjek	Status Liveness	Status *Liveness*	Status Pintu
1	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci

Pengujian	Kategori Subjek	Status Liveness	Status *Liveness*	Status Pintu
2	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
3	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
4	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
5	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
6	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
7	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
8	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
9	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
10	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
11	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
12	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
13	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
14	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
15	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
16	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Kategori Subjek	Status Liveness	Status *Liveness*	Status Pintu
17	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
18	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
19	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
20	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
21	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
22	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
23	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
24	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
25	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
26	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
27	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
28	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
29	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci
30	Spoofing Video	Terdeteksi Layar Video	Ditolak	Terkunci

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan rekaman log keamanan pada Tabel 4.17, pengujian gerbang pertahanan biometrik terhadap manipulasi rekaman video digital berhasil mencapai persentase pemblokiran mutlak sebesar 100%. Ketika lensa kamera menerima input visual dari layar ponsel pintar, model kecerdasan buatan secara responsif mengenali adanya ketidakwajaran struktur fisis objek dan mengeluarkan status "Terdeteksi Layar Video". Meskipun media video menampilkan pergerakan visual, sensor sistem mampu mengidentifikasi karakteristik khas media tiruan seperti pantulan cahaya (*glare*) dari lapisan kaca layar LCD/OLED, moiré pattern, serta ketiadaan informasi kedalaman ruang (*depth information*) yang murni milik manusia hidup. Kondisi indikasi kecurangan ini membuat program otomatis memutus aliran logika otentikasi, mengubah status tantangan interaksi menjadi "Ditolak", dan mempertahankan status pintu sepenuhnya aman "Terkunci".

4.4.3.4 Pengujian Akurasi Berdasarkan Jarak Deteksi

Pengujian ini dilakukan untuk mengevaluasi pengaruh variasi jarak fisik antara subjek pengguna dan kamera terhadap performa ekstraksi fitur wajah oleh model MobileFaceNet. Eksperimen terstruktur ini dilakukan secara bertahap pada jarak jangkau 40 cm, 60 cm, 80 cm, hingga 100 cm di bawah kondisi intensitas cahaya ruangan yang konstan (normal). Setiap skenario jarak diuji sebanyak 10 kali repetisi guna menganalisis stabilitas nilai kedekatan jarak vektor (*Cosine Score*), keberhasilan verifikasi *liveness detection*, serta konsistensi respon aktuator *solenoid door lock*. Hasil rekam data logistik dari keseluruhan pengujian jarak ini dirangkum secara sistematis pada tabel-tabel berikut.

a) Pengujian Jarak Deteksi 40 cm

Pengujian variasi jarak dilakukan untuk mengukur sensitivitas, akurasi, dan kecepatan sistem dalam mengenali wajah pengguna saat berdiri pada posisi yang berbeda di depan kamera. Perbedaan jarak memengaruhi ketajaman gambar wajah yang ditangkap oleh kamera Raspberry Pi, yang kemudian berdampak langsung pada nilai kemiripan (*Cosine Score*) serta waktu respon pemrosesan sistem. Sebagai langkah awal, pengujian dilakukan pada jarak operasional terbaik yaitu 40 cm guna melihat batas performa maksimal sistem dalam kondisi fokus yang paling ideal. Data hasil pengujian komprehensif dari 30 data wajah pada skenario jarak 40 cm disajikan secara detail pada Tabel 4.18.

Tabel 4.18 Pengujian Jarak Deteksi 40 cm

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Dikenali	Lolos	Terbuka	95,25%	162,2 ms	TP
2	Dikenali	Lolos	Terbuka	96,70%	176,8 ms	TP
3	Dikenali	Lolos	Terbuka	95,88%	165,6 ms	TP
4	Dikenali	Lolos	Terbuka	96,05%	172,4 ms	TP
5	Dikenali	Lolos	Terbuka	97,43%	169,5 ms	TP
6	Dikenali	Lolos	Terbuka	97,63%	168,6 ms	TP
7	Dikenali	Lolos	Terbuka	97,79%	168,4 ms	TP
8	Dikenali	Lolos	Terbuka	97,62%	157,2 ms	TP
9	Dikenali	Lolos	Terbuka	96,46%	168,3 ms	TP
10	Dikenali	Lolos	Terbuka	97,55%	172,6 ms	TP
11	Dikenali	Lolos	Terbuka	96,54%	162,6 ms	TP
12	Dikenali	Lolos	Terbuka	96,20%	164,5 ms	TP
13	Dikenali	Lolos	Terbuka	96,62%	174,0 ms	TP
14	Dikenali	Lolos	Terbuka	95,29%	170,7 ms	TP
15	Dikenali	Lolos	Terbuka	96,39%	168,3 ms	TP
16	Dikenali	Lolos	Terbuka	96,35%	162,9 ms	TP
17	Dikenali	Lolos	Terbuka	96,74%	160,3 ms	TP
18	Dikenali	Lolos	Terbuka	96,96%	176,0 ms	TP
19	Dikenali	Lolos	Terbuka	97,60%	167,1 ms	TP
20	Dikenali	Lolos	Terbuka	96,05%	168,7 ms	TP
21	Dikenali	Lolos	Terbuka	97,51%	163,0 ms	TP
22	Dikenali	Lolos	Terbuka	96,94%	157,8 ms	TP
23	Dikenali	Lolos	Terbuka	97,22%	160,5 ms	TP
24	Dikenali	Lolos	Terbuka	96,04%	168,1 ms	TP
25	Dikenali	Lolos	Terbuka	97,49%	160,1 ms	TP
26	Dikenali	Lolos	Terbuka	98,05%	165,5 ms	TP
27	Dikenali	Lolos	Terbuka	95,85%	169,1 ms	TP
28	Dikenali	Lolos	Terbuka	97,52%	167,1 ms	TP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
29	Dikenali	Lolos	Terbuka	95,88%	163,9 ms	TP
30	Dikenali	Lolos	Terbuka	97,18%	166,0 ms	TP
Rata – Rata				96,76%	166,6 ms	--

Berdasarkan data hasil eksperimen pada Tabel 4.18, pengujian pada skenario jarak 40 cm mencatatkan performa terbaik dengan tingkat keberhasilan mutlak 100% (True Positive) tanpa adanya kesalahan deteksi pada seluruh data wajah. Jarak 40 cm terbukti menjadi titik fokus kamera yang paling ideal bagi sistem, di mana seluruh data wajah berhasil Terdeteksi secara sempurna dan nilai kemiripan (*Cosine Score*) wajah pengguna yang sah mencapai rata-rata sangat tinggi sebesar 96,76%. Kualitas tangkapan gambar pada jarak ini memiliki kerapatan piksel yang sangat tajam, sehingga memudahkan kecerdasan buatan (*MobileFaceNet*) untuk mengenali lekukan dan karakteristik unik wajah secara mendetail dan akurat. Selain itu, ukuran area wajah yang pas di dalam layar mempercepat proses penyelarasan posisi titik wajah, yang menghasilkan kecepatan respon sistem sangat singkat dengan rata-rata waktu komputasi 166,6 ms. Dapat disimpulkan bahwa pada jarak operasional 40 cm, sistem mampu bekerja dengan sangat andal, cepat, dan aman dalam mendeteksi pengguna serta membuka akses pintu otomatis.

b) Pengujian Jarak Deteksi 60 cm

Pengujian pada skenario jarak 60 cm dilakukan untuk mengevaluasi konsistensi performa sistem ketika pengguna berada pada posisi sedikit lebih mundur dari titik ideal. Skenario ini mencerminkan kondisi penggunaan nyata di lapangan, di mana jarak berdiri pengguna cenderung dinamis dan bervariasi. Seluruh uji coba terhadap 30 data wajah ini diselenggarakan dalam kondisi lingkungan normal tanpa aksesoris wajah serta didukung oleh intensitas cahaya ruangan yang stabil. Data rekaman hasil pengujian secara menyeluruh disajikan pada Tabel 4.19.

Tabel 4.19 Pengujian Jarak Deteksi 60 cm

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Dikenali	Lolos	Terbuka	92,90%	217,7 ms	TP
2	Dikenali	Lolos	Terbuka	94,27%	211,4 ms	TP
3	Dikenali	Lolos	Terbuka	93,39%	210,8 ms	TP
4	Dikenali	Lolos	Terbuka	93,08%	222,0 ms	TP
5	Dikenali	Lolos	Terbuka	95,71%	217,5 ms	TP
6	Dikenali	Lolos	Terbuka	96,26%	207,5 ms	TP
7	Dikenali	Lolos	Terbuka	96,53%	199,2 ms	TP
8	Dikenali	Lolos	Terbuka	96,68%	198,8 ms	TP
9	Dikenali	Lolos	Terbuka	93,53%	221,2 ms	TP
10	Dikenali	Lolos	Terbuka	96,10%	215,5 ms	TP
11	Dikenali	Lolos	Terbuka	94,20%	217,4 ms	TP
12	Dikenali	Lolos	Terbuka	94,43%	225,2 ms	TP
13	Dikenali	Lolos	Terbuka	93,99%	201,1 ms	TP
14	Dikenali	Lolos	Terbuka	92,98%	218,1 ms	TP
15	Dikenali	Lolos	Terbuka	93,96%	215,5 ms	TP
16	Dikenali	Lolos	Terbuka	93,52%	217,2 ms	TP
17	Dikenali	Lolos	Terbuka	95,14%	205,9 ms	TP
18	Dikenali	Lolos	Terbuka	94,05%	218,6 ms	TP
19	Dikenali	Lolos	Terbuka	95,09%	191,5 ms	TP
20	Dikenali	Lolos	Terbuka	94,34%	215,7 ms	TP
21	Dikenali	Lolos	Terbuka	95,59%	214,4 ms	TP
22	Dikenali	Lolos	Terbuka	94,45%	224,2 ms	TP
23	Dikenali	Lolos	Terbuka	95,13%	204,4 ms	TP
24	Dikenali	Lolos	Terbuka	94,22%	215,6 ms	TP
25	Dikenali	Lolos	Terbuka	96,16%	200,4 ms	TP
26	Dikenali	Lolos	Terbuka	96,45%	197,3 ms	TP
27	Dikenali	Lolos	Terbuka	93,76%	213,3 ms	TP
28	Dikenali	Lolos	Terbuka	94,80%	211,4 ms	TP
29	Dikenali	Lolos	Terbuka	92,63%	213,7 ms	TP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
30	Dikenali	Lolos	Terbuka	95,14%	197,3 ms	TP
Rata – Rata				94,62%	211,3 ms	--

Berdasarkan data hasil eksperimen pada Tabel 4.3, pengujian pada skenario jarak 60 cm menunjukkan konsistensi performa yang sangat baik dengan tingkat keberhasilan pengenalan mencapai 100% (True Positive) untuk seluruh data wajah tanpa ada error deteksi. Seluruh data wajah tetap berhasil Terdeteksi dengan baik oleh sensor kamera, dan nilai kemiripan (*Cosine Score*) wajah pengguna yang sah berada pada kategori aman dengan rata-rata persentase sebesar 94,62% (di atas batas minimal *threshold* sistem yaitu 0,70). Terjadinya sedikit penurunan nilai kemiripan ini disebabkan oleh menyusutnya skala ukuran objek wajah pada sensor kamera yang mengurangi detail kerapatan piksel, namun model kecerdasan buatan (*MobileFaceNet*) terbukti masih sangat tangguh dalam mengekstraksi karakteristik wajah secara akurat. Dari aspek kecepatan respon, sistem membutuhkan rata-rata waktu komputasi selama 211,3 ms untuk menyelesaikan siklus pemindaian wajah. Waktu respon yang relatif singkat ini mengonfirmasi bahwa penambahan jarak sebesar 20 cm belum memberikan hambatan komputasi yang berarti bagi perangkat keras Raspberry Pi, sehingga sistem tetap responsif dalam membuka akses *smart door lock*.

c) Pengujian Jarak Deteksi 80 cm

Pengujian pada skenario jarak 80 cm ditujukan untuk memantau kestabilan identifikasi biometrik ketika jarak fisik antara subjek dan perangkat keras semakin merenggang. Evaluasi ini penting untuk mengetahui seberapa jauh model kecerdasan buatan mampu mempertahankan keakuratannya sebelum kualitas tangkapan kamera mengalami penurunan resolusi yang drastis. Seluruh uji coba terhadap 30 data wajah ini diselenggarakan dalam kondisi lingkungan normal tanpa penggunaan atribut wajah serta didukung oleh intensitas cahaya ruangan yang stabil. Data rekaman hasil pengujian secara menyeluruh disajikan pada Tabel 4.20.

Tabel 4.20 Pengujian Jarak Deteksi 80 cm

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Dikenali	Lolos	Terbuka	89,23%	268,9 ms	TP
2	Dikenali	Lolos	Terbuka	90,43%	260,2 ms	TP
3	Dikenali	Lolos	Terbuka	89,66%	252,0 ms	TP
4	Dikenali	Lolos	Terbuka	89,09%	256,1 ms	TP
5	Dikenali	Lolos	Terbuka	92,27%	272,0 ms	TP
6	Dikenali	Lolos	Terbuka	92,68%	249,7 ms	TP
7	Dikenali	Lolos	Terbuka	92,77%	265,6 ms	TP
8	Dikenali	Lolos	Terbuka	93,09%	265,0 ms	TP
9	Dikenali	Lolos	Terbuka	89,80%	271,2 ms	TP
10	Dikenali	Lolos	Terbuka	92,90%	252,8 ms	TP
11	Dikenali	Lolos	Terbuka	90,78%	248,7 ms	TP
12	Dikenali	Lolos	Terbuka	91,20%	270,4 ms	TP
13	Dikenali	Lolos	Terbuka	90,93%	264,3 ms	TP
14	Dikenali	Lolos	Terbuka	88,63%	273,0 ms	TP
15	Dikenali	Lolos	Terbuka	90,27%	257,0 ms	TP
16	Dikenali	Lolos	Terbuka	90,47%	265,4 ms	TP
17	Dikenali	Lolos	Terbuka	91,60%	242,9 ms	TP
18	Dikenali	Lolos	Terbuka	90,97%	273,8 ms	TP
19	Dikenali	Lolos	Terbuka	92,34%	256,3 ms	TP
20	Dikenali	Lolos	Terbuka	90,09%	261,6 ms	TP
21	Dikenali	Lolos	Terbuka	91,65%	263,4 ms	TP
22	Dikenali	Lolos	Terbuka	90,76%	252,7 ms	TP
23	Dikenali	Lolos	Terbuka	91,95%	252,5 ms	TP
24	Dikenali	Lolos	Terbuka	89,85%	274,4 ms	TP
25	Dikenali	Lolos	Terbuka	92,77%	267,2 ms	TP
26	Dikenali	Lolos	Terbuka	92,96%	254,4 ms	TP
27	Dikenali	Lolos	Terbuka	89,70%	260,3 ms	TP
28	Dikenali	Lolos	Terbuka	91,50%	263,5 ms	TP
29	Dikenali	Lolos	Terbuka	89,11%	269,7 ms	TP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
30	Dikenali	Lolos	Terbuka	91,80%	261,3 ms	TP
Rata – Rata				91,04%	261,5 ms	--

Berdasarkan data hasil eksperimen pada Tabel 4.20, pengujian pada skenario jarak 80 cm membuktikan bahwa sistem penguji tetap mempertahankan keandalan yang tinggi dengan persentase keberhasilan pengenalan mencapai 100% (True Positive) untuk seluruh data wajah tanpa ada error deteksi. Meskipun jarak fisik semakin merenggang, seluruh data wajah secara keseluruhan tetap sukses Terdeteksi oleh sistem. Akibat posisi objek wajah yang kian menjauh dari lensa kamera, nilai kemiripan (*Cosine Score*) wajah pengguna yang sah mengalami penurunan fisik secara bertahap hingga menyentuh nilai rata-rata 91,04%. Penurunan detail piksel kontur wajah ini menyebabkan sistem memerlukan waktu pemrosesan yang sedikit lebih lama untuk mencocokkan pola embeddings wajah, sehingga memicu peningkatan durasi respon rata-rata menjadi 261,5 ms. Kendati demikian, seluruh data uji coba masih dinilai sangat aman karena nilai rata-rata kemiripan tersebut tetap berada di atas batas minimal kelolosan (*threshold*) sistem yaitu 0,70, sehingga otentikasi biometrik berhasil dilakukan untuk membuka akses pintu otomatis.

d) Pengujian Jarak Deteksi 100 cm

Pengujian pada skenario jarak 100 cm (1 meter) diaplikasikan untuk menguji batas terjauh (*limit jangkauan*) dari sensor kamera dan efektivitas pembacaan algoritma biometrik wajah. Melalui penempatan jarak maksimal ini, dapat dianalisis titik kritis di mana performa sistem mulai mengalami penurunan akurasi atau perubahan status deteksi yang signifikan akibat keterbatasan resolusi gambar. Data logistik hasil pengujian dari 30 data wajah pada skenario jarak ekstrem 100 cm dituangkan secara lengkap dalam Tabel 4.21.

Tabel 4.21 Pengujian Jarak Deteksi 100 cm

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Dikenali	Lolos	Terbuka	80,67%	320,5 ms	TP

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
2	Dikenali	Lolos	Terbuka	81,78%	311,5 ms	TP
3	Dikenali	Lolos	Terbuka	79,75%	327,7 ms	TP
4	Dikenali	Lolos	Terbuka	79,85%	318,6 ms	TP
5	Dikenali	Lolos	Terbuka	84,57%	303,4 ms	TP
6	Dikenali	Lolos	Terbuka	85,38%	297,9 ms	TP
7	Dikenali	Lolos	Terbuka	85,70%	303,3 ms	TP
8	Dikenali	Lolos	Terbuka	87,90%	292,6 ms	TP
9	Dikenali	Lolos	Terbuka	82,31%	318,5 ms	TP
10	Salah dikenali	Lolos	Terbuka	82,98%	326,4 ms	FP
11	Dikenali	Lolos	Terbuka	84,01%	308,8 ms	TP
12	Dikenali	Lolos	Terbuka	83,51%	302,3 ms	TP
13	Dikenali	Lolos	Terbuka	83,65%	330,5 ms	TP
14	Dikenali	Lolos	Terbuka	79,68%	307,5 ms	TP
15	Dikenali	Lolos	Terbuka	81,43%	317,2 ms	TP
16	Dikenali	Lolos	Terbuka	81,65%	295,7 ms	TP
17	Dikenali	Lolos	Terbuka	84,53%	296,0 ms	TP
18	Dikenali	Lolos	Terbuka	83,95%	322,9 ms	TP
19	Dikenali	Lolos	Terbuka	84,86%	304,5 ms	TP
20	Tidak Dikenali	Lolos	Terkunci	66,26%	307,9 ms	FN
21	Dikenali	Lolos	Terbuka	83,93%	294,0 ms	TP
22	Dikenali	Lolos	Terbuka	83,29%	297,6 ms	TP
23	Dikenali	Lolos	Terbuka	85,10%	309,1 ms	TP
24	Dikenali	Lolos	Terbuka	81,15%	306,1 ms	TP
25	Dikenali	Lolos	Terbuka	86,37%	301,6 ms	TP
26	Dikenali	Lolos	Terbuka	86,77%	304,3 ms	TP
27	Dikenali	Lolos	Terbuka	79,68%	319,1 ms	TP
28	Dikenali	Lolos	Terbuka	84,14%	297,9 ms	TP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
29	Dikenali	Lolos	Terbuka	80,05%	312,3 ms	TP
30	Dikenali	Lolos	Terbuka	84,92%	301,5 ms	TP
Rata – Rata				82,66%	308,6 ms	--

Berdasarkan data hasil eksperimen pada Tabel 4.5, pengujian pada jarak batas maksimum 100 cm menunjukkan penurunan keandalan serta melambatnya performa komputasi sistem secara signifikan dibandingkan skenario jarak lainnya. Meskipun seluruh data wajah tetap berhasil Terdeteksi oleh kamera, rata-rata nilai kemiripan (*Cosine Score*) merosot ke angka 82,66% karena berkurangnya ketajaman guratan geometris wajah akibat posisi objek yang terlalu jauh. Penyusutan skala ukuran objek wajah ini juga memaksa prosesor Raspberry Pi membutuhkan waktu ekstra untuk memetakan koordinat citra, sehingga rata-rata waktu respon membengkak menjadi 308,6 ms. Hambatan fisik jarak ini menimbulkan anomali deteksi pada dua data wajah, yaitu kegagalan pengenalan (*False Negative*) pada sampel ke-20 karena skor kemiripan drop di bawah batas kelolosan (66,26%), serta kesalahan identifikasi nama (*False Positive*) pada sampel ke-10. Hal tersebut menegaskan bahwa jarak 100 cm merupakan ambang batas luar operasional (*limit jangkauan*) maksimal sistem sebelum akurasi kecerdasan buatan (*MobileFaceNet*) mengalami penurunan akurasi struktural akibat keterbatasan resolusi kamera.

4.4.3.5 Pengujian Ketahanan sistem

Pengujian ketahanan sistem dilakukan untuk mengevaluasi konsistensi serta keandalan performa algoritma *MobileFaceNet* saat dihadapkan pada berbagai hambatan fisik dan kondisi lingkungan ekstrem. Seluruh rangkaian pengujian pada tahap ini dilakukan secara konstan menggunakan parameter jarak operasional paling ideal, yaitu pada jarak 40 cm. Pemilihan jarak ideal 40 cm ini didasarkan pada hasil pengujian jarak sebelumnya (sebagaimana dirujuk pada data Tabel 4.18) yang terbukti memberikan tingkat akurasi murni (*Cosine Score*) tertinggi dan paling optimal sebesar 96,76%, di mana kerapatan piksel area wajah berada pada tingkat fokus kamera paling tajam. Pengujian ketahanan ini diskenariokan sebanyak 30 kali

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

pengujian untuk setiap parameter guna menguji batas toleransi sistem terhadap penghalangan atribut wajah (aksesoris) serta perubahan naik-turunnya intensitas pencahayaan ruangan.

A. Ketahanan Terhadap Aksesoris Wajah

Pengujian pada aspek halangan fisik (penutupan sebagian wajah) dilakukan untuk menguji sejauh mana keandalan sistem dalam mengekstrak serta memverifikasi fitur wajah ketika sebagian area wajah subjek terdaftar terhalang oleh aksesoris fisik. Pengujian ini diposisikan secara statis pada jarak terbaik 40 cm di bawah intensitas cahaya normal. Parameter kelayakan diukur berdasarkan kestabilan nilai kedekatan (*Cosine Score*), keberhasilan pemicuan tantangan keamanan, serta keputusan akhir status pembukaan pintu oleh sistem, yang dijabarkan secara detail sebagai berikut.

a) Skenario Penggunaan Topi

Pengujian ketahanan ini ditujukan untuk menilai seberapa tangguh sistem dalam mengenali karakteristik wajah pengguna ketika dahi dan sebagian rambut terhalang oleh aksesoris penutup kepala berupa topi. Eksperimen ini dilakukan secara konstan menggunakan parameter jarak ideal 40 cm untuk memastikan kerapatan piksel berada pada tingkat fokus kamera paling tajam. Data logistik hasil pengujian dari 30 data wajah pada skenario penggunaan topi disajikan secara detail pada Tabel 4.22.

Tabel 4.22 Skenario penggunaan Topi

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Dikenali	Lolos	Terbuka	85,80%	185,6 ms	TP
2	Dikenali	Lolos	Terbuka	87,44%	188,3 ms	TP
3	Dikenali	Lolos	Terbuka	86,33%	202,0 ms	TP
4	Dikenali	Lolos	Terbuka	86,29%	195,7 ms	TP
5	Dikenali	Lolos	Terbuka	88,33%	185,0 ms	TP
6	Dikenali	Lolos	Terbuka	89,22%	177,7 ms	TP
7	Dikenali	Lolos	Terbuka	88,54%	181,7 ms	TP
8	Dikenali	Lolos	Terbuka	88,78%	180,2 ms	TP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
9	Dikenali	Lolos	Terbuka	87,01%	185,3 ms	TP
10	Dikenali	Lolos	Terbuka	88,67%	192,5 ms	TP
11	Dikenali	Lolos	Terbuka	86,83%	202,4 ms	TP
12	Dikenali	Lolos	Terbuka	86,73%	205,0 ms	TP
13	Dikenali	Lolos	Terbuka	87,03%	192,8 ms	TP
14	Dikenali	Lolos	Terbuka	86,08%	209,7 ms	TP
15	Dikenali	Lolos	Terbuka	86,74%	195,5 ms	TP
16	Dikenali	Lolos	Terbuka	86,95%	194,4 ms	TP
17	Dikenali	Lolos	Terbuka	87,94%	199,0 ms	TP
18	Dikenali	Lolos	Terbuka	87,67%	198,7 ms	TP
19	Dikenali	Lolos	Terbuka	88,66%	174,8 ms	TP
20	Dikenali	Lolos	Terbuka	87,24%	193,2 ms	TP
21	Dikenali	Lolos	Terbuka	88,39%	187,1 ms	TP
22	Dikenali	Lolos	Terbuka	87,09%	184,5 ms	TP
23	Dikenali	Lolos	Terbuka	88,67%	195,2 ms	TP
24	Dikenali	Lolos	Terbuka	86,95%	203,7 ms	TP
25	Dikenali	Lolos	Terbuka	88,40%	190,9 ms	TP
26	Dikenali	Lolos	Terbuka	89,20%	196,9 ms	TP
27	Dikenali	Lolos	Terbuka	86,40%	209,9 ms	TP
28	Dikenali	Lolos	Terbuka	87,58%	195,1 ms	TP
29	Dikenali	Lolos	Terbuka	85,87%	192,2 ms	TP
30	Dikenali	Lolos	Terbuka	88,36%	190,7 ms	TP
Rata – Rata				87,51%	192,9 ms	--

Berdasarkan rekaman data pada Tabel 4.22, penggunaan aksesoris topi oleh subjek terdaftar pada jarak ideal 40 cm terbukti tidak mengganggu fungsionalitas utama sistem biometrik. Dari 30 kali pengujian yang dilakukan, sistem secara konsisten berhasil mengenali identitas masing-masing subjek dan membuka kunci pintu dengan tingkat keberhasilan mutlak 100% (True Positive). Struktur *neural network* pada *MobileFaceNet* mampu mempertahankan akurasi pencatatan matriks dengan

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

nilai *Cosine Score* yang stabil pada rentang minimal 85,80% hingga maksimal 89,22%, sehingga menghasilkan rata-rata kumulatif sebesar 87,51%. Meskipun nilai kemiripan ini mengalami penurunan (*degradasi*) dibandingkan kondisi normal tanpa aksesoris karena tertutupnya area dahi, perolehannya masih berada jauh di atas nilai *threshold* aman sistem sebesar 0,70. Hal ini dikarenakan bagian wajah krusial sebagai titik acuan biometrik utama seperti mata, hidung, dan mulut tidak tertutup oleh topi, sehingga algoritma tetap responsif mengeksekusi data secara lancar dengan rata-rata respon wajah singkat selama 192,9 ms hingga pintu berhasil terbuka.

b) Skenario Penggunaan Kacamata

Pengujian ketahanan ini ditujukan untuk menilai sensitivitas kamera dan model dalam memetakan area orbital (mata) pengguna ketika terhalang oleh lensa atau bingkai kacamata bening. Eksperimen ini dilakukan secara konstan menggunakan parameter jarak ideal 40 cm untuk memastikan kerapatan piksel berada pada tingkat fokus kamera paling tajam. Data logistik hasil pengujian dari 30 data wajah pada skenario penggunaan kacamata bening disajikan secara detail pada Tabel 4.23.

Tabel 4.23 Skenario Pengggunaan Kacamata

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Dikenali	Lolos	Terbuka	77,21%	205,3 ms	TP
2	Dikenali	Lolos	Terbuka	79,05%	210,6 ms	TP
3	Dikenali	Lolos	Terbuka	77,69%	202,4 ms	TP
4	Dikenali	Lolos	Terbuka	77,51%	209,3 ms	TP
5	Dikenali	Lolos	Terbuka	81,28%	197,9 ms	TP
6	Dikenali	Lolos	Terbuka	81,73%	203,2 ms	TP
7	Dikenali	Lolos	Terbuka	81,51%	203,4 ms	TP
8	Dikenali	Lolos	Terbuka	82,37%	192,7 ms	TP
9	Dikenali	Lolos	Terbuka	78,16%	194,2 ms	TP
10	Dikenali	Lolos	Terbuka	81,61%	203,0 ms	TP
11	Dikenali	Lolos	Terbuka	79,24%	205,6 ms	TP
12	Dikenali	Lolos	Terbuka	79,19%	192,7 ms	TP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
13	Dikenali	Lolos	Terbuka	79,74%	191,9 ms	TP
14	Dikenali	Lolos	Terbuka	77,28%	194,9 ms	TP
15	Dikenali	Lolos	Terbuka	79,26%	208,5 ms	TP
16	Dikenali	Lolos	Terbuka	78,37%	201,0 ms	TP
17	Dikenali	Lolos	Terbuka	80,32%	185,4 ms	TP
18	Dikenali	Lolos	Terbuka	79,87%	204,3 ms	TP
19	Dikenali	Lolos	Terbuka	81,60%	208,2 ms	TP
20	Dikenali	Lolos	Terbuka	78,54%	215,8 ms	TP
21	Dikenali	Lolos	Terbuka	81,10%	191,6 ms	TP
22	Dikenali	Lolos	Terbuka	79,46%	210,2 ms	TP
23	Dikenali	Lolos	Terbuka	80,81%	204,3 ms	TP
24	Dikenali	Lolos	Terbuka	78,92%	200,4 ms	TP
25	Dikenali	Lolos	Terbuka	81,45%	180,5 ms	TP
26	Dikenali	Lolos	Terbuka	82,42%	185,0 ms	TP
27	Dikenali	Lolos	Terbuka	78,16%	204,6 ms	TP
28	Dikenali	Lolos	Terbuka	80,96%	201,4 ms	TP
29	Dikenali	Lolos	Terbuka	76,99%	217,8 ms	TP
30	Dikenali	Lolos	Terbuka	81,28%	190,3 ms	TP
Rata – Rata				79,77%	200,5 ms	--

Berdasarkan rekaman data pada Tabel 4.23, penggunaan aksesoris kacamata bening oleh subjek terdaftar pada jarak ideal 40 cm menunjukkan bahwa sistem tetap sukses mencapai tingkat keberhasilan pembukaan pintu 100% (True Positive) untuk seluruh data wajah tanpa ada error deteksi. Dari 30 kali pengujian yang dilakukan, struktur *neural network* pada *MobileFaceNet* mampu mempertahankan akurasi pencatatan matriks dengan nilai *Cosine Score* yang stabil pada rentang minimal 76,99% hingga maksimal 82,42%, sehingga menghasilkan rata-rata kumulatif sebesar 79,77%. Penurunan nilai kemiripan murni ini disebabkan oleh refleksi cahaya pada permukaan lensa kacamata bening serta hambatan fisik dari bingkai (*frame*) kacamata yang mengaburkan sebagian bentuk geometris mata dan pangkal

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

hidung subjek. Kendati demikian, seluruh data uji coba masih dinilai sangat aman karena nilai rata-rata kemiripan tersebut terbukti masih melampaui batas minimal kelolosan (*threshold*) sistem sebesar 0,70, sehingga perangkat keras Raspberry Pi tetap bekerja responsif mengeksekusi data dengan rata-rata respon wajah singkat selama 200,5 ms hingga pintu berhasil terbuka.

c) Skenario Penggunaan Masker

Pengujian ketahanan ini ditujukan untuk mengevaluasi batasan toleransi sistem biometrik ketika sebagian besar area wajah pengguna meliputi hidung, pipi bawah, mulut, hingga dagu tertutup oleh atribut masker medis. Eksperimen ini dilakukan secara konstan menggunakan parameter jarak ideal 40 cm untuk memastikan kerapatan piksel berada pada tingkat fokus kamera paling tajam. Data logistik hasil pengujian dari 30 data wajah pada skenario penggunaan masker disajikan secara detail pada Tabel 4.24.

Tabel 4.24 Skenario Penggunaan Masker

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Tidak Dikenali	Terhalang	Terkunci	24,82%	236,3 ms	TN
2	Tidak Dikenali	Terhalang	Terkunci	24,15%	243,1 ms	TN
3	Tidak Dikenali	Terhalang	Terkunci	26,72%	269,3 ms	TN
4	Tidak Dikenali	Terhalang	Terkunci	21,14%	277,4 ms	TN
5	Tidak Dikenali	Terhalang	Terkunci	24,93%	249,0 ms	TN
6	Tidak Dikenali	Terhalang	Terkunci	31,26%	251,9 ms	TN
7	Tidak Dikenali	Terhalang	Terkunci	28,16%	235,6 ms	TN

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
8	Tidak Dikenali	Terhalang	Terkunci	31,07%	249,5 ms	TN
9	Tidak Dikenali	Terhalang	Terkunci	24,97%	273,0 ms	TN
10	Tidak Dikenali	Terhalang	Terkunci	26,28%	267,5 ms	TN
11	Tidak Dikenali	Terhalang	Terkunci	23,20%	259,2 ms	TN
12	Tidak Dikenali	Terhalang	Terkunci	29,02%	244,9 ms	TN
13	Tidak Dikenali	Terhalang	Terkunci	28,48%	240,4 ms	TN
14	Tidak Dikenali	Terhalang	Terkunci	23,13%	235,8 ms	TN
15	Tidak Dikenali	Terhalang	Terkunci	29,85%	268,5 ms	TN
16	Tidak Dikenali	Terhalang	Terkunci	20,85%	262,2 ms	TN
17	Tidak Dikenali	Terhalang	Terkunci	28,00%	272,8 ms	TN
18	Tidak Dikenali	Terhalang	Terkunci	27,12%	272,3 ms	TN
19	Tidak Dikenali	Terhalang	Terkunci	29,95%	249,0 ms	TN
20	Tidak Dikenali	Terhalang	Terkunci	27,34%	228,0 ms	TN
21	Tidak Dikenali	Terhalang	Terkunci	30,25%	273,3 ms	TN
22	Tidak Dikenali	Terhalang	Terkunci	30,59%	277,8 ms	TN

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
23	Tidak Dikenali	Terhalang	Terkunci	26,94%	225,2 ms	TN
24	Tidak Dikenali	Terhalang	Terkunci	24,66%	276,8 ms	TN
25	Tidak Dikenali	Terhalang	Terkunci	31,01%	236,5 ms	TN
26	Tidak Dikenali	Terhalang	Terkunci	32,75%	247,1 ms	TN
27	Tidak Dikenali	Terhalang	Terkunci	25,17%	268,0 ms	TN
28	Tidak Dikenali	Terhalang	Terkunci	30,95%	244,1 ms	TN
29	Tidak Dikenali	Terhalang	Terkunci	26,95%	248,5 ms	TN
30	Tidak Dikenali	Terhalang	Terkunci	29,58%	246,5 ms	TN
Rata – Rata				27,31%	254,3 ms	--

Berdasarkan rekaman data pada Tabel 4.24, penggunaan aksesoris masker oleh subjek terdaftar pada jarak ideal 40 cm secara konsisten memicu penolakan sistem dengan tingkat keberhasilan mutlak dalam mengamankan pintu dari wajah terhalang sebesar 100% True Negative (TN). Dari 30 kali pengujian yang disimulasikan, sistem secara akurat mempertahankan status pintu tetap Terkunci dan menolak akses masuk karena algoritma *MobileFaceNet* mencatatkan penurunan nilai kemiripan (*Cosine Score*) yang sangat drastis pada rentang minimal 20,85% hingga maksimal 32,75%, sehingga menghasilkan rata-rata kumulatif hanya sebesar 27,31%. Penurunan tajam ini berada jauh di bawah nilai *threshold* aman sistem sebesar 0,70 karena masker menutupi lebih dari separuh komponen struktural wajah krusial yang berfungsi sebagai parameter ekstraksi vektor fitur utama, sehingga sistem memerlukan rata-rata waktu pemrosesan (*Respon Wajah*)

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

selama 254,3 ms untuk memastikan validasi embeddings wajah sebelum akhirnya menolak otentikasi demi menjaga keamanan *smart door lock*.

B. Ketahanan Terhadap Intensitas Cahaya Ekstrem

Pengujian ini dilakukan untuk melihat batas toleransi dan keandalan sensor kamera serta algoritma *MobileFaceNet* saat beroperasi di luar kondisi pencahayaan ideal (normal). Seluruh pengujian pada tahap ini diposisikan secara konsisten menggunakan jarak operasional paling ideal, yaitu 40 cm. Skenario pengujian difokuskan pada dua kondisi ekstrem yang sering ditemui di lapangan, yaitu kondisi minim cahaya (*lowlight*) dan kondisi bayangan latar kuat (*backlight*).

a) Skenario Kondisi *Lowlight*

Pengujian ketahanan ini ditujukan untuk mengevaluasi konsistensi dan batas kemampuan adaptasi sensor kamera serta algoritma dalam mengenali wajah pengguna pada kondisi pencahayaan yang minim (lowlight). Eksperimen ini dilakukan secara konstan menggunakan parameter jarak ideal 40 cm untuk memastikan kerapatan piksel berada pada tingkat fokus kamera paling tajam. Data logistik hasil pengujian dari 30 data wajah pada skenario kondisi kurang cahaya (lowlight) disajikan secara detail pada Tabel 4.25.

Tabel 4.25 Skenario Kondisi *Lowlight*

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Dikenali	Lolos	Terbuka	69,75%	349,7 ms	TP
2	Tidak Dikenali	Lolos	Terkunci	64,15%	377,7 ms	FN
3	Dikenali	Lolos	Terbuka	71,21%	324,2 ms	TP
4	Dikenali	Lolos	Terbuka	70,67%	351,8 ms	TP
5	Dikenali	Lolos	Terbuka	77,23%	361,2 ms	TP
6	Dikenali	Lolos	Terbuka	78,78%	333,3 ms	TP
7	Dikenali	Lolos	Terbuka	79,56%	348,9 ms	TP
8	Dikenali	Lolos	Terbuka	80,17%	368,1 ms	TP
9	Dikenali	Lolos	Terbuka	71,75%	338,2 ms	TP

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
10	Dikenali	Lolos	Terbuka	78,33%	354,2 ms	TP
11	Dikenali	Lolos	Terbuka	74,11%	360,9 ms	TP
12	Tidak Dikenali	Lolos	Terkunci	62,93%	353,4 ms	FN
13	Dikenali	Lolos	Terbuka	73,74%	353,0 ms	TP
14	Dikenali	Lolos	Terbuka	69,57%	325,8 ms	TP
15	Dikenali	Lolos	Terbuka	72,87%	333,0 ms	TP
16	Dikenali	Lolos	Terbuka	71,76%	379,8 ms	TP
17	Dikenali	Lolos	Terbuka	75,69%	367,4 ms	TP
18	Dikenali	Lolos	Terbuka	74,67%	368,3 ms	TP
19	Dikenali	Lolos	Terbuka	77,87%	323,6 ms	TP
20	Dikenali	Lolos	Terbuka	72,27%	324,4 ms	TP
21	Dikenali	Lolos	Terbuka	75,70%	376,6 ms	TP
22	Salah Dikenali	Lolos	Terbuka	72,17%	344,6 ms	FP
23	Dikenali	Lolos	Terbuka	77,23%	326,4 ms	TP
24	Dikenali	Lolos	Terbuka	72,16%	332,3 ms	TP
25	Dikenali	Lolos	Terbuka	78,46%	379,0 ms	TP
26	Dikenali	Lolos	Terbuka	79,78%	346,1 ms	TP
27	Dikenali	Lolos	Terbuka	71,54%	338,9 ms	TP
28	Dikenali	Lolos	Terbuka	76,58%	366,4 ms	TP
29	Dikenali	Lolos	Terbuka	69,55%	348,2 ms	TP
30	Dikenali	Lolos	Terbuka	77,15%	378,7 ms	TP
Rata – Rata				73,91%	351,1 ms	--

Berdasarkan rekaman data pada Tabel 4.25, pengujian ketahanan terhadap intensitas cahaya minim (*lowlight*) pada jarak ideal 40 cm memicu penurunan performa akurasi yang cukup terlihat akibat berkurangnya pencahayaan pada sensor kamera. Kondisi minim pencahayaan ini memicu penurunan kontras piksel dan memunculkan *noise* visual pada lensa kamera, sehingga nilai kedekatan *Cosine*

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Score merosot ke rentang terendah 62,93% hingga nilai tertinggi 80,17%, dengan pencapaian nilai rata-rata aktual sistem berada di angka 73,91%. Penurunan kualitas visual akibat kegelapan ini menyebabkan sistem mengalami anomali deteksi pada tiga sampel uji, yaitu kegagalan pengenalan pengguna terdaftar (*False Negative*) pada pengujian ke-2 dan ke-12 karena skor berada di bawah batas kelolosan aman sistem sebesar 0,67, serta kesalahan identifikasi nama (*False Positive*) pada pengujian ke-22. Keterbatasan intensitas cahaya ini juga memaksa prosesor Raspberry Pi bekerja lebih keras dalam mencari titik landmark wajah, sehingga waktu komputasi (*Respon Wajah*) melambat secara signifikan dengan rata-rata latensi mencapai 351,1 ms sebelum berhasil mengeksekusi perintah kunci pintu.

b) Skenario Kondisi *Backlight*

Pengujian ketahanan ini ditujukan untuk mengevaluasi konsistensi serta performa algoritma *MobileFaceNet* saat dihadapkan pada gangguan kontras visual berupa efek cahaya latar (*backlight*). Kondisi ini mensimulasikan situasi di mana sumber cahaya yang kuat berada tepat di belakang subjek, sehingga berpotensi menggelapkan siluet area wajah bagian depan. Seluruh rangkaian pengujian pada tahap ini dilakukan secara konstan menggunakan parameter jarak operasional paling ideal, yaitu pada jarak 40 cm. Data logistik hasil pengujian dari 30 data wajah pada skenario efek cahaya latar (*backlight*) disajikan secara detail pada Tabel 4.26.

Tabel 4.26 Skenario Kondisi *Backlight*

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
1	Dikenali	Lolos	Terbuka	66,90%	345,8 ms	TP
2	Dikenali	Lolos	Terbuka	70,26%	396,6 ms	TP
3	Dikenali	Lolos	Terbuka	68,36%	387,9 ms	TP
4	Dikenali	Lolos	Terbuka	67,48%	333,1 ms	TP
5	Tidak Dikenali	Lolos	Terkunci	61,14%	353,2 ms	FN
6	Dikenali	Lolos	Terbuka	76,19%	362,3 ms	TP
7	Dikenali	Lolos	Terbuka	74,69%	367,2 ms	TP
8	Dikenali	Lolos	Terbuka	76,66%	392,9 ms	TP

Pengujian	Identitas	Liveness	Status	Cosine Score	Respon Wajah	keterangan
9	Dikenali	Lolos	Terbuka	69,33%	394,8 ms	TP
10	Dikenali	Lolos	Terbuka	74,51%	357,7 ms	TP
11	Dikenali	Lolos	Terbuka	71,33%	356,6 ms	TP
12	Dikenali	Lolos	Terbuka	70,69%	368,7 ms	TP
13	Dikenali	Lolos	Terbuka	70,70%	348,8 ms	TP
14	Dikenali	Lolos	Terbuka	67,57%	342,4 ms	TP
15	Dikenali	Lolos	Terbuka	69,92%	332,1 ms	TP
16	Salah Dikenali	Lolos	Terbuka	76,75%	348,6 ms	FP
17	Dikenali	Lolos	Terbuka	73,14%	344,3 ms	TP
18	Dikenali	Lolos	Terbuka	71,90%	356,7 ms	TP
19	Dikenali	Lolos	Terbuka	74,21%	334,2 ms	TP
20	Dikenali	Lolos	Terbuka	70,35%	363,1 ms	TP
21	Dikenali	Lolos	Terbuka	73,66%	349,7 ms	TP
22	Dikenali	Lolos	Terbuka	70,96%	386,4 ms	TP
23	Dikenali	Lolos	Terbuka	74,46%	348,5 ms	TP
24	Dikenali	Lolos	Terbuka	70,09%	340,3 ms	TP
25	Tidak Dikenali	Lolos	Terkunci	62,47%	336,5 ms	FN
26	Dikenali	Lolos	Terbuka	75,72%	375,4 ms	TP
27	Dikenali	Lolos	Terbuka	68,06%	367,8 ms	TP
28	Dikenali	Lolos	Terbuka	73,12%	399,1 ms	TP
29	Dikenali	Lolos	Terbuka	67,90%	370,9 ms	TP
30	Dikenali	Lolos	Terbuka	72,75%	355,3 ms	TP
Rata – Rata				71,04%	360,6 ms	--

Berdasarkan rekaman data pada Tabel 4.26, pengujian ketahanan terhadap gangguan pencahayaan berlebih dari belakang objek (*backlight*) pada jarak ideal 40 cm memicu degradasi visual yang cukup signifikan pada area deteksi wajah pengguna terdaftar. Hadirnya sumber cahaya kuat yang membelakangi subjek ini

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

memicu penurunan kontras piksel dan menggelapkan detail karakteristik wajah di depan lensa kamera, sehingga nilai kedekatan *Cosine Score* merosot ke rentang terendah 61,14% hingga nilai tertinggi 76,75%, dengan pencapaian nilai rata-rata aktual sistem berada di angka 71,04%. Efek siluet gelap akibat paparan cahaya latar ini menyebabkan sistem mengalami anomali identifikasi pada tiga sampel uji, yaitu kegagalan pengenalan (*False Negative*) pada pengujian ke-5 dan ke-25 karena skor jatuh di bawah batas kelolosan minimal 0,65, serta kesalahan identifikasi nama (*False Positive*) pada pengujian ke-16. Hambatan iluminasi ini juga memaksa modul ekstraksi fitur bekerja ekstra keras dalam memetakan pola koordinat wajah, sehingga waktu komputasi (*Respon Wajah*) melambat secara signifikan dengan rata-rata durasi aktual mencapai 360,6 ms sebelum berhasil mengeksekusi perintah otentikasi kunci pintu.

4.4.3.6 Pengujian Klasifikasi Biometrik

Setelah melaksanakan seluruh rangkaian eksperimen pengujian terhadap 270 sampel data aktual di lapangan, tahapan selanjutnya adalah melakukan rekapitulasi data hasil pengujian untuk mengukur performa sistem secara matematis. Pengujian komprehensif ini mengintegrasikan model *MobileFaceNet* dengan parameter variasi jarak serta pengujian ketahanan atribut dan lingkungan yang seluruh proses komputasinya dieksekusi secara lokal pada perangkat Raspberry Pi. Pengujian ini melibatkan pengamatan terhadap kondisi wajah yang terdaftar dan dikenali, serta pengujian ketahanan sistem dalam mengenali kondisi terhalang (seperti pada penggunaan masker) atau penyusup. Melalui pengelompokan hasil ke dalam tabel kontingensi *Confusion Matrix*, performa kecerdasan buatan pada sistem ini dapat dievaluasi secara terukur melalui empat metrik standar, yaitu Akurasi (*Accuracy*), Presisi (*Precision*), Sensitivitas (*Recall*), dan *F1-Score*.

a) Tabel Hasil Pengujian

Berdasarkan akumulasi data mentah dari total seluruh rangkaian pengujian terhadap 30 data wajah yang disimulasikan ke dalam 9 skenario berbeda, sebaran distribusi keputusan sistem dirangkum ke dalam Tabel 4.27 di bawah ini:

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Table 4.27 Hasil Pengujian

Sampel Wajah	Terdeteksi Pengguna Sah	Terdeteksi Orang Asing
Pengguna Sah (Kondisi Ideal & Tantangan)	TP = 232	FN = 5
Kondisi Terhalang / Masker	FP = 3	TN a= 30

Berdasarkan data pada Tabel 4.27, pengujian kelompok identitas pengguna sah menghasilkan 232 sampel True Positive (TP), di mana wajah terdaftar sukses dikenali secara akurat oleh *MobileFaceNet* sehingga pintu berhasil terbuka (*UNLOCKED*). Adapun 5 sampel False Negative (FN) yang terjadi disebabkan oleh kondisi ekstrem jarak jauh 100 cm (1 sampel), kondisi redup/lowlight (2 sampel), dan kondisi cahaya latar/backlight (2 sampel) yang membuat sistem gagal memvalidasi wajah terdaftar akibat penurunan drastis kualitas citra.

Sementara itu, sistem mencatatkan 30 sampel True Negative (TN) sempurna pada skenario masker, yang membuktikan keandalan sistem dalam menolak akses ketika wajah dalam kondisi terhalang penuh. Terdapat pula 3 sampel False Positive (FP) (1 sampel pada jarak 100 cm, 1 sampel pada lowlight, dan 1 sampel pada backlight) di mana sistem mengalami salah identifikasi nama akibat keterbatasan pencahayaan dan resolusi fisik kamera.

b) Hasil Perhitungan Metrik

Melalui nilai parameter sebaran yang diperoleh dari Tabel 4.11 (TP = 232, FN = 5, TN = 30, FP = 3), dilakukan kalkulasi menggunakan rumus matematis untuk mendapatkan nilai persentase performa akhir dari model AI sistem:

Tabel 4.28 Perhitungan Metrik

Metrik Evaluasi	Variabel Input	Hasil Akhir %
Akurasi (*Accuracy*)	$\frac{TP + TN}{TP + TN + FP + FN}$	97,04%
Presisi (*Precision*)	$\frac{TP}{TP + FP}$	98,72%
Sensitivitas (*Recall*)	$\frac{TP}{TP + FN}$	97,89%

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Metrik Evaluasi	Variabel Input	Hasil Akhir %
F1-Score	$2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$	98,31%

Dari hasil kalkulasi pada Tabel 4.28, nilai Akurasi global diperoleh sebesar 97,04%, yang berarti keputusan klasifikasi biometrik berhasil dieksekusi dengan tepat sebanyak 262 kali dari total 270 percobaan di berbagai skenario ekstrem. Sistem mencatatkan nilai Presisi yang sangat tinggi yaitu 98,72% yang membuktikan bahwa tingkat kesalahan klasifikasi positif palsu (*False Positive*) sangat minim terjadi meski sistem ditekan pada kondisi ruangan gelap maupun siluet cahaya.

Sementara itu, nilai Sensitivitas (*Recall*) berada di angka 97,89% karena hanya terdapat 5 kali kondisi penolakan palsu (*False Negative*). Sebagai kesimpulan, capaian akhir nilai rata-rata harmonis F1-Score berada pada tingkat persentase sebesar 98,31%, yang menunjukkan efisiensi kinerja model *MobileFaceNet* pada sistem *smart door lock* ini berjalan dengan sangat optimal, seimbang, dan andal di lapangan.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian sistem *smart door lock* berbasis *Edge Computing* menggunakan Raspberry Pi 4 Model B, maka dapat disimpulkan sebagai berikut:

1. Hasil Implementasi sistem *smart door lock* berbasis IoT telah berhasil dibangun pada perangkat Raspberry Pi 4 Model B dan terbukti andal mencegah akses tidak sah. Penerapan metode *liveness detection* memiliki tingkat keberhasilan 100% dalam mengenali dan menolak semua bentuk pemalsuan wajah, baik menggunakan foto cetak maupun rekaman video di ponsel.
2. Berdasarkan hasil pengujian model AI MobileFaceNet memiliki ketangguhan solid dengan akurasi global 97,04%, presisi 98,72%, sensitivitas 97,89%, dan F1-Score 98,31%, di mana pada jarak optimal 40 cm sistem mampu mempertahankan rata-rata *Cosine Score* sebesar 96,76% pada pencahayaan normal, 73,91% pada kondisi minim cahaya (*low-light*), dan 71,04% pada kondisi cahaya latar (*backlight*).

5.2 Saran

Berdasarkan seluruh rangkaian tahapan penelitian, implementasi, dan evaluasi yang telah dilakukan terhadap sistem *smart door lock*, berikut beberapa saran yang dapat dijadikan acuan untuk pengembangan sistem selanjutnya:

1. Perlu dilakukan optimasi pada algoritma ekstraksi fitur agar dapat meningkatkan kembali nilai kemiripan (*Cosine Score*) pengguna sah yang menurun akibat penggunaan kacamata atau topi, serta pengembangan *threshold* adaptif agar sistem ke depannya tetap mampu mengenali pengguna sah meskipun sedang menggunakan masker.
2. Disarankan untuk menambahkan perangkat keras pencahayaan tambahan, seperti lampu LED atau sensor inframerah pada sirkuit alat, guna menstabilkan kualitas tangkapan kamera dan menjaga nilai pencocokan wajah pada kondisi lingkungan yang sangat gelap atau siluet.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

Ahwadti, R. D., & Setiawan, A. P. (2025). Sistem Keamanan Pintu Rumah Menggunakan Face Recognition Berbasis IoT. *Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB)*, 1081-1088.

Algabri, R., Abdu, A., & Lee, S. (2024). Deep learning and machine learning techniques for head pose estimation: a survey. *Artificial Intelligence Review*, *57*, 288. https://doi.org/10.1007/s10462-024-10936-7

Anwar, M. K., & Sugiantoro, B. (2026). Comparison of Deep Learning Architectures for Facial Recognition. *Dinasti International Journal of Education Management and Social Science (DIJEMSS)*, *7*(3), 3237-3247.

Asperti, A., & Filippini, D. (2023). Deep Learning for Head Pose Estimation: A Survey. *SN Computer Science*, *4*, 349. https://doi.org/10.1007/s42979-023-01796-z

Bazarevsky, V., Kartynnik, Y., Vakunov, A., Raveendran, K., & Grundmann, M. (2019). BlazeFace: Sub-millisecond Neural Face Detection on Mobile GPUs. *arXiv preprint arXiv:1907.05047v2*.

Chakraborty, A., Islam, M., Shahriyar, F., Islam, S., Zaman, H. U., & Hasan, M. (2023). Smart Home System: A Comprehensive Review. *Journal of Electrical and Computer Engineering*, *2023*, 7616683. https://doi.org/10.1155/2023/7616683

Chuah, W.-H., Chong, S.-C., & Chong, L.-Y. (2023). The Assistance of Eye Blink Detection for Two-Factor Authentication. *Journal of Informatics and Web Engineering*, *2*(2), 111-121. https://doi.org/10.33093/jiwe.2023.2.2.8

Daher, A. W., Rizik, A., Muselli, M., Chible, H., & Caviglia, D. D. (2021). Porting Rulex Software to the Raspberry Pi for Machine Learning Applications on the Edge. *Sensors*, *21*(19), 6526. https://doi.org/10.3390/s21196526

Dewi, C., Chen, R.-C., Jiang, X., & Yu, H. (2022). Adjusting eye aspect ratio for strong eye blink detection based on facial landmarks. *PeerJ Computer Science*, *8*, e943. https://doi.org/10.7717/peerj-cs.943

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Dewi, N., & Ismawan, F. (2021). Implementasi Deep Learning Menggunakan Convolutional Neural Network untuk Sistem Pengenalan Wajah. *Faktor Exacta*, *14*(1), 34-43. https://doi.org/10.30998/faktorexacta.v14i1.8989

Fernando, B., Sridhar, A., Talebi, S., Waczak, J., & Lary, D. J. (2022). Unsupervised Blink Detection Using Eye Aspect Ratio Values. *Preprints*. https://doi.org/10.20944/preprints202203.0200.v1

Fitriani Dewi, E. N., Tarempa, G. N., Rachman, A. N., & Febriansyah, A. (2025). Sistem Presensi Perkuliahan Mahasiswa Berbasis Face Recognition dengan Metode Liveness Detection. *Indonesian Journal Computer Science*, *4*(2), 118-126.

George, A., & Marcel, S. (2021). On the Effectiveness of Vision Transformers for Zero-shot Face Anti-Spoofing. *Idiap Research Institute*.

George, A., Geissbühler, D., & Marcel, S. (2022). A Comprehensive Evaluation on Multi-channel Biometric Face Presentation Attack Detection. *arXiv preprint arXiv:2202.10286v1*.

Harbi, Y., Aliouat, Z., Refoufi, A., & Harous, S. (2021). Recent Security Trends in Internet of Things: A Comprehensive Survey. *IEEE Access*, *9*, 1-23.

Harke, N., Patil, A., Nimbalkar, Y., Khore, S., & Rathod, S. (2022). Smart Door Lock System Using Face Recognition. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *10*(5), 3111-3113.

Hermawan, I., Agustin, M., Zain, A. R., Mulyani, M. T., & Nathanael, D. (2023). Rice Seedling Image Classification Using Light Convolutional Neural Network. *Khazanah Informatika: Jurnal Ilmu Komputer dan Informatika*, *9*(2), 111-118.

Kartynnik, Y., Ablavatski, A., Grishchenko, I., & Grundmann, M. (2019). Real-time Facial Surface Geometry from Monocular Video on Mobile GPUs. *arXiv preprint arXiv:1907.06724v1*.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Kiarie, G., Kabi, J., & wa Maina, C. (2022). DSAIL power management board: Powering the Raspberry Pi autonomously off the grid. *HardwareX*, *12*, e00337.

Liu, W., Zhou, L., & Chen, J. (2021). Face Recognition Based on Lightweight Convolutional Neural Networks. *Information*, *12*(5), 191. https://doi.org/10.3390/info12050191

Liu, X., Wu, B., Yuan, X., & Yi, X. (n.d.). Leia: A Lightweight Cryptographic Neural Network Inference System at the Edge. *IEEE Transactions on Information Forensics and Security*.

Luriansyah, R. P., Nugraha, D. A., & Harianto, W. (2022). Sistem Pengenalan Wajah pada Keamanan Pintu Otomatis Menggunakan Metode Eigenface Berbasis Raspberry Pi. *KURAWAL: Jurnal Teknologi, Informasi dan Industri*, *5*(2), 98-103.

Makama, I., & Gana, S. M. (2021). Design and Implementation of Home Automation System Based on Raspberry Pi. *NIPES Journal of Science and Technology Research*, *3*(4), 125-134. https://doi.org/10.37933/nipes/3.4.2021.13

Maulana, I., Azriadi, E., & Musridho, R. J. (2023). Rancang Bangun Sistem Smart Door Lock Menggunakan Mikrokontroler Esp32 Berbasis Internet Of Things (IoT) dan Smartphone Android. *JUTIN: Jurnal Teknik Industri Terintegrasi*, *6*(1), 195-208. https://doi.org/10.31004/jutin.v6i1.15123

Nur, M., Sulistyowati, H. S., & Nurrohman, A. (2024). Penerapan Face Recognition untuk Model Smart Lock Door Berbasis IoT. *Jurnal Tridi: Teknologi Informatika & Komputer*, *2*(1), 152-157.

Rofiq, A., Wagyana, A., & Junianto, P. D. (2024). Perancangan dan Implementasi Sistem Smart Locker dengan Face Recognition Berbasis Internet of Things. *Spektral: Journal of Communications, Antennas and Propagation*, *5*(1), 239-245.

Šćepanović, I., & Šćepanović, V. (2022). Does smart home have wide open doors? MQTT communication protocol standardization - potential missing ring of the IoT networks security chain. *Social Informatics Journal*, *1*(1), 23-29.

Soedjarwanto, N., Nama, G. F., & Nugroho, R. A. (2021). Prototipe Smart Door Lock Menggunakan Motor Stepper Berbasis IoT (Internet of Things). *ELECTRICIAN - Jurnal Rekayasa dan Teknologi Elektro*, *15*(2), 74-82.

Wijaya, A. M., Samodra, J. E., & Suyoto. (2023). Sistem Presensi Pegawai dengan Face Recognition Menggunakan Deep Learning CNN. *Jurnal Informatika Atma Jogja*, *4*(2), 163-168.

Xu, X., Du, M., Guo, H., Chang, J., & Zhao, X. (2021). Lightweight FaceNet Based on MobileNet. *International Journal of Intelligence Science*, *11*, 1-16. https://doi.org/10.4236/ijis.2021.111001

Yanto, B., Basorudin, Anwar, S., Lubis, A., & Karmi. (2022). Smart Home Monitoring Pintu Rumah dengan Identifikasi Wajah Menerapkan Camera ESP32 Berbasis IoT. *Jurnal SISFOKOM (Sistem Informasi dan Komputer)*, *11*(1), 53-59. https://doi.org/10.32736/sisfokom.v11i1.1180

Yu, Z., Qin, Y., Li, X., Zhao, C., Lei, Z., & Zhao, G. (2022). Deep Learning for Face Anti-Spoofing: A Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.

Zhang, S., & Nie, W. (2023). Multi-Domain Feature Alignment for Face Anti-Spoofing. *Sensors*, *23*(8), 4077. https://doi.org/10.3390/s23084077

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR RIWAYAT HIDUP

Fahrul Rosi

Lahir di Palembang pada tahun 2003, Merupakan anak kedua dari dua bersaudara, berdomisili di Kota Depok. Lulus pendidikan dasar di SDN Pasar Manggris 03 pada tahun 2016. Kemudian melanjutkan pendidikan menengah pertama di SMP Negeri 280 Jakarta dan lulus pada tahun 2019. Kemudian melanjutkan pendidikan menengah atas di SMA Negeri 3 Jakarta dan lulus pada tahun 2022. Kemudian melanjutkan pendidikan sebagai mahasiswa Diploma Empat (D4) Politeknik Negeri Jakarta (PNJ) dengan jurusan Teknik Informatika dan Komputer dengan prodi Teknik Multimedia dan Jaringan.

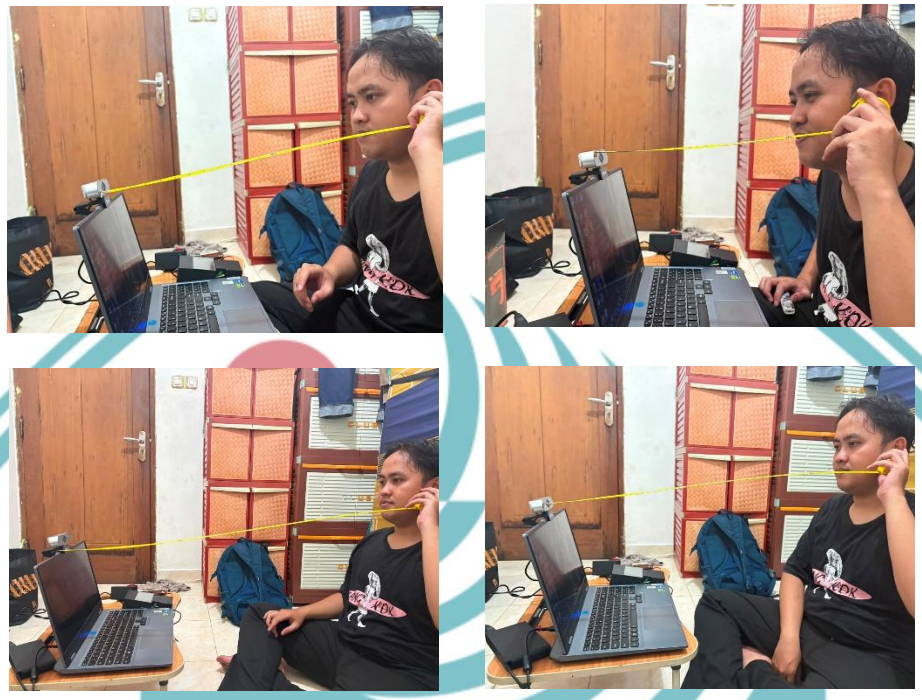
POLITEKNIK NEGERI JAKARTA

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LAMPIRAN

Lampiran 1. Pengujian Jarak



Lampiran 2. Pengujian Ketahanan Menggunakan Aksesoris

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 3. Data Pengujian *Preprocessing*

No	Nama	Status Pose (ms)	Blink Buka (ms)	Blink Tutup (ms)	Blink Total (ms)	Latensi (ms)
1	Wak Alex	313,4	271,3	213,5	484,8	3635,8
2	Bu ade	683,1	479,2	304,1	783,3	3333,2
3	Risma	344,8	386,8	256,8	643,6	2806,1
4	Vira	4022,9	211,6	1301,5	1513,1	9036,5
5	Pak Yadi	279,7	400,3	218,6	618,9	3274,8
6	Nanda	586,5	380,5	299,2	679,7	3507,5
7	Suleha	203,9	339,6	262,2	601,8	2904,5
8	Mpok Pepen	556,4	359,8	255,5	615,3	4072,7
9	Kakek Rosi	325,8	292,8	274,3	567,1	3783,4
10	Fahrul Rosi	3801,6	371,0	2670,9	3041,9	15777,0
11	Widia	547,0	304,5	205,5	510,0	2915,3
12	Bang ijal	387,0	456,2	306,6	762,8	3041,2
13	Kenny	205,8	255,4	269,6	525,0	3196,4
14	Mpok Lia	232,9	433,6	160,6	594,2	2727,1
15	Holijah	672,7	277,4	177,6	455,0	3993,1
16	Aprilia	478,4	266,7	202,7	469,4	3860,1
17	Andin	542,7	407,1	251,9	659,0	3143,9
18	Andini	344,1	312,6	292,4	605,0	3470,8
19	Miftah	288,0	440,9	341,3	782,2	3040,8
20	Joni	736,1	300,7	171,2	471,9	3301,4
21	Ayah Ganis	207,1	421,1	212,5	633,6	3748,4
22	Mursal	247,7	331,6	268,3	599,9	3662,9
23	Aji	623,0	394,4	219,0	613,4	3865,9
24	Anjani	468,4	368,6	288,1	656,7	3260,0
25	Erlan	209,8	433,8	183,7	617,5	2893,4
26	Julian	261,2	359,8	263,1	622,9	4180,8
27	Rajib	521,6	309,4	174,1	483,5	3406,7
28	Aulia	494,6	289,4	317,1	606,5	2988,0
29	Martini	522,1	305,9	174,3	480,2	3674,0
30	Pak Tio	405,9	409,6	307,3	716,9	3402,9
	Rata-rata	**650,5**	**352,4**	**361,5**	**713,8**	**3996,8**

Lampiran 4. Data Pengujian Jarak 40, 60, 80, dan 100

TABEL HASIL PENGUJIAN - SKENARIO: JARAK 40CM

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Dikenali (Fahrul Rosi)	Lolos	Terbuka	95,25%	162,2 ms	True Positive (TP)
2	Dikenali (Vira)	Lolos	Terbuka	96,70%	176,8 ms	True Positive (TP)
3	Dikenali (Aji)	Lolos	Terbuka	95,88%	165,6 ms	True Positive (TP)
4	Dikenali (Andin)	Lolos	Terbuka	96,05%	172,4 ms	True Positive (TP)
5	Dikenali (Andini)	Lolos	Terbuka	97,43%	169,5 ms	True Positive (TP)
6	Dikenali (Anjani)	Lolos	Terbuka	97,63%	168,6 ms	True Positive (TP)
7	Dikenali (Aprilia)	Lolos	Terbuka	97,79%	168,4 ms	True Positive (TP)
8	Dikenali (Aulia)	Lolos	Terbuka	97,62%	157,2 ms	True Positive (TP)
9	Dikenali (Ayah Ganis)	Lolos	Terbuka	96,46%	168,3 ms	True Positive (TP)
10	Dikenali (Bang ijal)	Lolos	Terbuka	97,55%	172,6 ms	True Positive (TP)
11	Dikenali (Bu ade)	Lolos	Terbuka	96,54%	162,6 ms	True Positive (TP)
12	Dikenali (Erlan)	Lolos	Terbuka	96,20%	164,5 ms	True Positive (TP)
13	Dikenali (Holijah)	Lolos	Terbuka	96,62%	174,0 ms	True Positive (TP)
14	Dikenali (Joni)	Lolos	Terbuka	95,29%	170,7 ms	True Positive (TP)
15	Dikenali (Julian)	Lolos	Terbuka	96,39%	168,3 ms	True Positive (TP)
16	Dikenali (Kakek Rosi)	Lolos	Terbuka	96,35%	162,9 ms	True Positive (TP)
17	Dikenali (Kenny)	Lolos	Terbuka	96,74%	160,3 ms	True Positive (TP)
18	Dikenali (Martini)	Lolos	Terbuka	96,96%	176,0 ms	True Positive (TP)
19	Dikenali (Miftah)	Lolos	Terbuka	97,60%	167,1 ms	True Positive (TP)
20	Dikenali (Mpok Lia)	Lolos	Terbuka	96,05%	168,7 ms	True Positive (TP)
21	Dikenali (Mpok Pepen)	Lolos	Terbuka	97,51%	163,0 ms	True Positive (TP)
22	Dikenali (Mursal)	Lolos	Terbuka	96,94%	157,8 ms	True Positive (TP)
23	Dikenali (Nanda)	Lolos	Terbuka	97,22%	160,5 ms	True Positive (TP)
24	Dikenali (Pak Tio)	Lolos	Terbuka	96,04%	168,1 ms	True Positive (TP)
25	Dikenali (Pak Yadi)	Lolos	Terbuka	97,49%	160,1 ms	True Positive (TP)
26	Dikenali (Rajib)	Lolos	Terbuka	98,05%	165,5 ms	True Positive (TP)
27	Dikenali (Risma)	Lolos	Terbuka	95,85%	169,1 ms	True Positive (TP)
28	Dikenali (Suleha)	Lolos	Terbuka	97,52%	167,1 ms	True Positive (TP)
29	Dikenali (Wak Alex)	Lolos	Terbuka	95,88%	163,9 ms	True Positive (TP)
30	Dikenali (Widia)	Lolos	Terbuka	97,18%	166,0 ms	True Positive (TP)
Rata - Rata				**96,76%**	**166,6 ms**	–

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

TABEL HASIL PENGUJIAN - SKENARIO: JARAK 60CM

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Dikenali (Fahrul Rosi)	Lolos	Terbuka	92,90%	217,7 ms	True Positive (TP)
2	Dikenali (Vira)	Lolos	Terbuka	94,27%	211,4 ms	True Positive (TP)
3	Dikenali (Aji)	Lolos	Terbuka	93,39%	210,8 ms	True Positive (TP)
4	Dikenali (Andin)	Lolos	Terbuka	93,08%	222,0 ms	True Positive (TP)
5	Dikenali (Andini)	Lolos	Terbuka	95,71%	217,5 ms	True Positive (TP)
6	Dikenali (Anjani)	Lolos	Terbuka	96,26%	207,5 ms	True Positive (TP)
7	Dikenali (Aprilia)	Lolos	Terbuka	96,53%	199,2 ms	True Positive (TP)
8	Dikenali (Aulia)	Lolos	Terbuka	96,68%	198,8 ms	True Positive (TP)
9	Dikenali (Ayah Ganis)	Lolos	Terbuka	93,53%	221,2 ms	True Positive (TP)
10	Dikenali (Bang ijal)	Lolos	Terbuka	96,10%	215,5 ms	True Positive (TP)
11	Dikenali (Bu ade)	Lolos	Terbuka	94,20%	217,4 ms	True Positive (TP)
12	Dikenali (Erlan)	Lolos	Terbuka	94,43%	225,2 ms	True Positive (TP)
13	Dikenali (Hollijah)	Lolos	Terbuka	93,93%	201,1 ms	True Positive (TP)
14	Dikenali (Joni)	Lolos	Terbuka	92,98%	218,1 ms	True Positive (TP)
15	Dikenali (Julian)	Lolos	Terbuka	93,96%	215,5 ms	True Positive (TP)
16	Dikenali (Kakek Rosi)	Lolos	Terbuka	93,52%	217,2 ms	True Positive (TP)
17	Dikenali (Kenny)	Lolos	Terbuka	95,14%	205,3 ms	True Positive (TP)
18	Dikenali (Martini)	Lolos	Terbuka	94,05%	218,6 ms	True Positive (TP)
19	Dikenali (Miftah)	Lolos	Terbuka	95,09%	191,5 ms	True Positive (TP)
20	Dikenali (Mpok Lia)	Lolos	Terbuka	94,34%	215,7 ms	True Positive (TP)
21	Dikenali (Mpok Pepen)	Lolos	Terbuka	95,59%	214,4 ms	True Positive (TP)
22	Dikenali (Mursal)	Lolos	Terbuka	94,45%	224,2 ms	True Positive (TP)
23	Dikenali (Nanda)	Lolos	Terbuka	95,13%	204,4 ms	True Positive (TP)
24	Dikenali (Pak Tio)	Lolos	Terbuka	94,22%	215,6 ms	True Positive (TP)
25	Dikenali (Pak Yadi)	Lolos	Terbuka	96,16%	200,4 ms	True Positive (TP)
26	Dikenali (Rajib)	Lolos	Terbuka	96,45%	197,3 ms	True Positive (TP)
27	Dikenali (Risma)	Lolos	Terbuka	93,76%	213,3 ms	True Positive (TP)
28	Dikenali (Suleha)	Lolos	Terbuka	94,80%	211,4 ms	True Positive (TP)
29	Dikenali (Wak Alex)	Lolos	Terbuka	92,63%	213,7 ms	True Positive (TP)
30	Dikenali (Widia)	Lolos	Terbuka	95,14%	197,3 ms	True Positive (TP)
Rata - Rata				**94,62%**	**211,3 ms**	–

TABEL HASIL PENGUJIAN – SKENARIO: JARAK 80CM

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Dikenali (Fahrul Rosi)	Lolos	Terbuka	89,23%	268,9 ms	True Positive (TP)
2	Dikenali (Vira)	Lolos	Terbuka	90,43%	260,2 ms	True Positive (TP)
3	Dikenali (Aji)	Lolos	Terbuka	89,66%	252,0 ms	True Positive (TP)
4	Dikenali (Andin)	Lolos	Terbuka	89,09%	256,1 ms	True Positive (TP)
5	Dikenali (Andini)	Lolos	Terbuka	92,27%	272,0 ms	True Positive (TP)
6	Dikenali (Anjani)	Lolos	Terbuka	92,68%	249,7 ms	True Positive (TP)
7	Dikenali (Aprilia)	Lolos	Terbuka	92,77%	265,6 ms	True Positive (TP)
8	Dikenali (Aulia)	Lolos	Terbuka	93,09%	265,0 ms	True Positive (TP)
9	Dikenali (Ayah Ganis)	Lolos	Terbuka	89,80%	271,2 ms	True Positive (TP)
10	Dikenali (Bang ijal)	Lolos	Terbuka	92,90%	252,8 ms	True Positive (TP)
11	Dikenali (Bu ade)	Lolos	Terbuka	90,78%	248,7 ms	True Positive (TP)
12	Dikenali (Erlan)	Lolos	Terbuka	91,20%	270,4 ms	True Positive (TP)
13	Dikenali (Hollijah)	Lolos	Terbuka	90,93%	264,3 ms	True Positive (TP)
14	Dikenali (Joni)	Lolos	Terbuka	88,63%	273,0 ms	True Positive (TP)
15	Dikenali (Julian)	Lolos	Terbuka	90,27%	257,0 ms	True Positive (TP)
16	Dikenali (Kakek Rosi)	Lolos	Terbuka	90,47%	265,4 ms	True Positive (TP)
17	Dikenali (Kenny)	Lolos	Terbuka	91,60%	242,9 ms	True Positive (TP)
18	Dikenali (Martini)	Lolos	Terbuka	90,97%	273,8 ms	True Positive (TP)
19	Dikenali (Miftah)	Lolos	Terbuka	92,34%	256,3 ms	True Positive (TP)
20	Dikenali (Mpok Lia)	Lolos	Terbuka	90,09%	261,6 ms	True Positive (TP)
21	Dikenali (Mpok Pepen)	Lolos	Terbuka	91,65%	263,4 ms	True Positive (TP)
22	Dikenali (Mursal)	Lolos	Terbuka	90,76%	252,7 ms	True Positive (TP)
23	Dikenali (Nanda)	Lolos	Terbuka	91,95%	252,5 ms	True Positive (TP)
24	Dikenali (Pak Tio)	Lolos	Terbuka	89,85%	274,4 ms	True Positive (TP)
25	Dikenali (Pak Yadi)	Lolos	Terbuka	92,77%	267,2 ms	True Positive (TP)
26	Dikenali (Rajib)	Lolos	Terbuka	92,96%	254,4 ms	True Positive (TP)
27	Dikenali (Risma)	Lolos	Terbuka	89,70%	260,3 ms	True Positive (TP)
28	Dikenali (Suleha)	Lolos	Terbuka	91,50%	263,5 ms	True Positive (TP)
29	Dikenali (Wak Alex)	Lolos	Terbuka	89,11%	269,7 ms	True Positive (TP)
30	Dikenali (Widia)	Lolos	Terbuka	91,80%	261,3 ms	True Positive (TP)
Rata - Rata				**91,04%**	**261,5 ms**	–

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

TABEL HASIL PENGUJIAN - SKENARIO: JARAK 100CM

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Dikenali (Fahrul Rosi)	Lolos	Terbuka	80,67%	320,5 ms	True Positive (TP)
2	Dikenali (Vira)	Lolos	Terbuka	81,78%	311,5 ms	True Positive (TP)
3	Dikenali (Aji)	Lolos	Terbuka	79,75%	327,7 ms	True Positive (TP)
4	Dikenali (Andin)	Lolos	Terbuka	79,85%	318,6 ms	True Positive (TP)
5	Dikenali (Andini)	Lolos	Terbuka	84,57%	303,4 ms	True Positive (TP)
6	Dikenali (Anjani)	Lolos	Terbuka	85,38%	297,9 ms	True Positive (TP)
7	Dikenali (Aprilia)	Lolos	Terbuka	85,70%	303,3 ms	True Positive (TP)
8	Dikenali (Aulia)	Lolos	Terbuka	87,90%	292,6 ms	True Positive (TP)
9	Dikenali (Ayah Ganis)	Lolos	Terbuka	82,31%	318,5 ms	True Positive (TP)
10	Teridentifikasi Salah (Bang ijal)	Lolos	Terbuka	82,98%	326,4 ms	False Positive (FP)
11	Dikenali (Bu ade)	Lolos	Terbuka	84,01%	308,8 ms	True Positive (TP)
12	Dikenali (Erlan)	Lolos	Terbuka	83,51%	302,3 ms	True Positive (TP)
13	Dikenali (Holijah)	Lolos	Terbuka	83,65%	330,5 ms	True Positive (TP)
14	Dikenali (Joni)	Lolos	Terbuka	79,68%	307,5 ms	True Positive (TP)
15	Dikenali (Julian)	Lolos	Terbuka	81,43%	317,2 ms	True Positive (TP)
16	Dikenali (Kakek Rosi)	Lolos	Terbuka	81,65%	295,7 ms	True Positive (TP)
17	Dikenali (Kenny)	Lolos	Terbuka	84,53%	296,0 ms	True Positive (TP)
18	Dikenali (Martini)	Lolos	Terbuka	83,95%	322,9 ms	True Positive (TP)
19	Dikenali (Miftah)	Lolos	Terbuka	84,86%	304,5 ms	True Positive (TP)
20	Tidak Dikenali	Lolos	Terkunci	66,26%	307,9 ms	False Negative (FN)
21	Dikenali (Mpok Pepen)	Lolos	Terbuka	83,93%	294,0 ms	True Positive (TP)
22	Dikenali (Mursal)	Lolos	Terbuka	83,29%	297,6 ms	True Positive (TP)
23	Dikenali (Nanda)	Lolos	Terbuka	85,10%	309,1 ms	True Positive (TP)
24	Dikenali (Pak Tio)	Lolos	Terbuka	81,15%	306,1 ms	True Positive (TP)
25	Dikenali (Pak Yadi)	Lolos	Terbuka	86,37%	301,6 ms	True Positive (TP)
26	Dikenali (Rajib)	Lolos	Terbuka	86,77%	304,3 ms	True Positive (TP)
27	Dikenali (Risma)	Lolos	Terbuka	79,68%	319,1 ms	True Positive (TP)
28	Dikenali (Suleha)	Lolos	Terbuka	84,14%	297,9 ms	True Positive (TP)
29	Dikenali (Wak Alex)	Lolos	Terbuka	80,05%	312,3 ms	True Positive (TP)
30	Dikenali (Widia)	Lolos	Terbuka	84,92%	301,5 ms	True Positive (TP)
Rata - Rata				**82,66%**	**308,6 ms**	–

Lampiran 5. Data Pengujian Menggunakan Aksesoris Seperti

TABEL HASIL PENGUJIAN - SKENARIO: TOPI

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Dikenali (Fahrul Rosi)	Lolos	Terbuka	85,80%	185,6 ms	True Positive (TP)
2	Dikenali (Vira)	Lolos	Terbuka	87,44%	188,3 ms	True Positive (TP)
3	Dikenali (Aji)	Lolos	Terbuka	86,33%	202,0 ms	True Positive (TP)
4	Dikenali (Andin)	Lolos	Terbuka	86,29%	195,7 ms	True Positive (TP)
5	Dikenali (Andini)	Lolos	Terbuka	88,33%	185,0 ms	True Positive (TP)
6	Dikenali (Anjani)	Lolos	Terbuka	89,22%	177,7 ms	True Positive (TP)
7	Dikenali (Aprilia)	Lolos	Terbuka	88,54%	181,7 ms	True Positive (TP)
8	Dikenali (Aulia)	Lolos	Terbuka	88,78%	180,2 ms	True Positive (TP)
9	Dikenali (Ayah Ganis)	Lolos	Terbuka	87,01%	185,3 ms	True Positive (TP)
10	Dikenali (Bang ijal)	Lolos	Terbuka	88,67%	192,5 ms	True Positive (TP)
11	Dikenali (Bu ade)	Lolos	Terbuka	86,83%	202,4 ms	True Positive (TP)
12	Dikenali (Erlan)	Lolos	Terbuka	86,73%	205,0 ms	True Positive (TP)
13	Dikenali (Holijah)	Lolos	Terbuka	87,03%	192,8 ms	True Positive (TP)
14	Dikenali (Joni)	Lolos	Terbuka	86,08%	209,7 ms	True Positive (TP)
15	Dikenali (Julian)	Lolos	Terbuka	86,74%	195,5 ms	True Positive (TP)
16	Dikenali (Kakek Rosi)	Lolos	Terbuka	86,95%	194,4 ms	True Positive (TP)
17	Dikenali (Kenny)	Lolos	Terbuka	87,94%	199,0 ms	True Positive (TP)
18	Dikenali (Martini)	Lolos	Terbuka	87,67%	198,7 ms	True Positive (TP)
19	Dikenali (Miftah)	Lolos	Terbuka	88,66%	174,8 ms	True Positive (TP)
20	Dikenali (Mpok Lia)	Lolos	Terbuka	87,24%	193,2 ms	True Positive (TP)
21	Dikenali (Mpok Pepen)	Lolos	Terbuka	88,39%	187,1 ms	True Positive (TP)
22	Dikenali (Mursal)	Lolos	Terbuka	87,09%	184,5 ms	True Positive (TP)
23	Dikenali (Nanda)	Lolos	Terbuka	88,67%	195,2 ms	True Positive (TP)
24	Dikenali (Pak Tio)	Lolos	Terbuka	86,95%	203,7 ms	True Positive (TP)
25	Dikenali (Pak Yadi)	Lolos	Terbuka	88,40%	190,9 ms	True Positive (TP)
26	Dikenali (Rajib)	Lolos	Terbuka	89,20%	196,9 ms	True Positive (TP)
27	Dikenali (Risma)	Lolos	Terbuka	86,40%	209,9 ms	True Positive (TP)
28	Dikenali (Suleha)	Lolos	Terbuka	87,58%	195,1 ms	True Positive (TP)
29	Dikenali (Wak Alex)	Lolos	Terbuka	85,87%	192,2 ms	True Positive (TP)
30	Dikenali (Widia)	Lolos	Terbuka	88,36%	190,7 ms	True Positive (TP)
Rata - Rata				**87,51%**	**192,9 ms**	–

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

TABEL HASIL PENGUJIAN – SKENARIO: KACAMATA

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Dikenali (Fahrul Rosi)	Lolos	Terbuka	77,21%	205,3 ms	True Positive (TP)
2	Dikenali (Vira)	Lolos	Terbuka	79,05%	210,6 ms	True Positive (TP)
3	Dikenali (Aji)	Lolos	Terbuka	77,69%	202,4 ms	True Positive (TP)
4	Dikenali (Andin)	Lolos	Terbuka	77,51%	203,3 ms	True Positive (TP)
5	Dikenali (Andini)	Lolos	Terbuka	81,28%	197,9 ms	True Positive (TP)
6	Dikenali (Anjani)	Lolos	Terbuka	81,73%	203,2 ms	True Positive (TP)
7	Dikenali (Aprilia)	Lolos	Terbuka	81,51%	203,4 ms	True Positive (TP)
8	Dikenali (Aulia)	Lolos	Terbuka	82,37%	192,7 ms	True Positive (TP)
9	Dikenali (Ayah Ganis)	Lolos	Terbuka	78,16%	194,2 ms	True Positive (TP)
10	Dikenali (Bang ijal)	Lolos	Terbuka	81,61%	203,0 ms	True Positive (TP)
11	Dikenali (Bu ade)	Lolos	Terbuka	79,24%	205,6 ms	True Positive (TP)
12	Dikenali (Erlan)	Lolos	Terbuka	79,13%	192,7 ms	True Positive (TP)
13	Dikenali (Holijah)	Lolos	Terbuka	79,74%	191,9 ms	True Positive (TP)
14	Dikenali (Joni)	Lolos	Terbuka	77,28%	194,9 ms	True Positive (TP)
15	Dikenali (Julian)	Lolos	Terbuka	79,26%	208,5 ms	True Positive (TP)
16	Dikenali (Kakek Rosi)	Lolos	Terbuka	78,37%	201,0 ms	True Positive (TP)
17	Dikenali (Kenny)	Lolos	Terbuka	80,32%	185,4 ms	True Positive (TP)
18	Dikenali (Martini)	Lolos	Terbuka	79,87%	204,3 ms	True Positive (TP)
19	Dikenali (Miftah)	Lolos	Terbuka	81,60%	208,2 ms	True Positive (TP)
20	Dikenali (Mpok Lia)	Lolos	Terbuka	78,54%	215,8 ms	True Positive (TP)
21	Dikenali (Mpok Popen)	Lolos	Terbuka	81,10%	191,6 ms	True Positive (TP)
22	Dikenali (Mursal)	Lolos	Terbuka	79,46%	210,2 ms	True Positive (TP)
23	Dikenali (Nanda)	Lolos	Terbuka	80,81%	204,3 ms	True Positive (TP)
24	Dikenali (Pak Tio)	Lolos	Terbuka	78,32%	200,4 ms	True Positive (TP)
25	Dikenali (Pak Yadi)	Lolos	Terbuka	81,45%	180,5 ms	True Positive (TP)
26	Dikenali (Rajib)	Lolos	Terbuka	82,42%	185,0 ms	True Positive (TP)
27	Dikenali (Risma)	Lolos	Terbuka	78,16%	204,6 ms	True Positive (TP)
28	Dikenali (Sulcha)	Lolos	Terbuka	80,36%	201,4 ms	True Positive (TP)
29	Dikenali (Wak Alex)	Lolos	Terbuka	76,93%	217,8 ms	True Positive (TP)
30	Dikenali (Widia)	Lolos	Terbuka	81,28%	190,3 ms	True Positive (TP)
Rata - Rata				79,77%	200,5 ms	—

TABEL HASIL PENGUJIAN - SKENARIO: MASKER

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Tidak Dikenali	Terhalang	Terkunci	24,82%	236,3 ms	True Negative (TN)
2	Tidak Dikenali	Terhalang	Terkunci	24,15%	243,1 ms	True Negative (TN)
3	Tidak Dikenali	Terhalang	Terkunci	26,72%	269,3 ms	True Negative (TN)
4	Tidak Dikenali	Terhalang	Terkunci	21,14%	277,4 ms	True Negative (TN)
5	Tidak Dikenali	Terhalang	Terkunci	24,93%	249,0 ms	True Negative (TN)
6	Tidak Dikenali	Terhalang	Terkunci	31,26%	251,9 ms	True Negative (TN)
7	Tidak Dikenali	Terhalang	Terkunci	28,16%	235,6 ms	True Negative (TN)
8	Tidak Dikenali	Terhalang	Terkunci	31,07%	249,5 ms	True Negative (TN)
9	Tidak Dikenali	Terhalang	Terkunci	24,97%	273,0 ms	True Negative (TN)
10	Tidak Dikenali	Terhalang	Terkunci	26,28%	267,5 ms	True Negative (TN)
11	Tidak Dikenali	Terhalang	Terkunci	23,20%	259,2 ms	True Negative (TN)
12	Tidak Dikenali	Terhalang	Terkunci	29,02%	244,9 ms	True Negative (TN)
13	Tidak Dikenali	Terhalang	Terkunci	28,48%	240,4 ms	True Negative (TN)
14	Tidak Dikenali	Terhalang	Terkunci	23,13%	235,8 ms	True Negative (TN)
15	Tidak Dikenali	Terhalang	Terkunci	29,85%	268,5 ms	True Negative (TN)
16	Tidak Dikenali	Terhalang	Terkunci	20,85%	262,2 ms	True Negative (TN)
17	Tidak Dikenali	Terhalang	Terkunci	28,00%	272,8 ms	True Negative (TN)
18	Tidak Dikenali	Terhalang	Terkunci	27,12%	272,3 ms	True Negative (TN)
19	Tidak Dikenali	Terhalang	Terkunci	29,95%	249,0 ms	True Negative (TN)
20	Tidak Dikenali	Terhalang	Terkunci	27,34%	228,0 ms	True Negative (TN)
21	Tidak Dikenali	Terhalang	Terkunci	30,25%	273,3 ms	True Negative (TN)
22	Tidak Dikenali	Terhalang	Terkunci	30,59%	277,8 ms	True Negative (TN)
23	Tidak Dikenali	Terhalang	Terkunci	26,94%	225,2 ms	True Negative (TN)
24	Tidak Dikenali	Terhalang	Terkunci	24,66%	276,8 ms	True Negative (TN)
25	Tidak Dikenali	Terhalang	Terkunci	31,01%	236,5 ms	True Negative (TN)
26	Tidak Dikenali	Terhalang	Terkunci	32,75%	247,1 ms	True Negative (TN)
27	Tidak Dikenali	Terhalang	Terkunci	25,17%	268,0 ms	True Negative (TN)
28	Tidak Dikenali	Terhalang	Terkunci	30,95%	244,1 ms	True Negative (TN)
29	Tidak Dikenali	Terhalang	Terkunci	26,95%	248,5 ms	True Negative (TN)
30	Tidak Dikenali	Terhalang	Terkunci	29,58%	246,5 ms	True Negative (TN)
Rata - Rata				27,31%	254,3 ms	—

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 6. Data Pengujian Pencahayaan *Lowlight* dan *Backlight*

TABEL HASIL PENGUJIAN - SKENARIO: LOWLIGHT

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Dikenali (Fahrul Rosi)	Lolos	Terbuka	69,75%	349,7 ms	True Positive (TP)
2	Tidak Dikenali	Lolos	Terkunci	64,15%	377,7 ms	False Negative (FN)
3	Dikenali (Aji)	Lolos	Terbuka	71,21%	324,2 ms	True Positive (TP)
4	Dikenali (Andin)	Lolos	Terbuka	70,67%	351,8 ms	True Positive (TP)
5	Dikenali (Andini)	Lolos	Terbuka	77,23%	361,2 ms	True Positive (TP)
6	Dikenali (Anjani)	Lolos	Terbuka	78,78%	333,3 ms	True Positive (TP)
7	Dikenali (Aprilia)	Lolos	Terbuka	79,56%	348,9 ms	True Positive (TP)
8	Dikenali (Aulia)	Lolos	Terbuka	80,17%	368,1 ms	True Positive (TP)
9	Dikenali (Ayah Ganis)	Lolos	Terbuka	71,75%	338,2 ms	True Positive (TP)
10	Dikenali (Bang ijal)	Lolos	Terbuka	78,33%	354,2 ms	True Positive (TP)
11	Dikenali (Bu ade)	Lolos	Terbuka	74,11%	360,9 ms	True Positive (TP)
12	Tidak Dikenali	Lolos	Terkunci	62,93%	353,4 ms	False Negative (FN)
13	Dikenali (Holijah)	Lolos	Terbuka	73,74%	353,0 ms	True Positive (TP)
14	Dikenali (Joni)	Lolos	Terbuka	69,57%	325,8 ms	True Positive (TP)
15	Dikenali (Julian)	Lolos	Terbuka	72,87%	333,0 ms	True Positive (TP)
16	Dikenali (Kakek Rosi)	Lolos	Terbuka	71,76%	379,8 ms	True Positive (TP)
17	Dikenali (Kenny)	Lolos	Terbuka	75,69%	367,4 ms	True Positive (TP)
18	Dikenali (Martini)	Lolos	Terbuka	74,67%	368,3 ms	True Positive (TP)
19	Dikenali (Miftah)	Lolos	Terbuka	77,87%	323,6 ms	True Positive (TP)
20	Dikenali (Mpok Lia)	Lolos	Terbuka	72,27%	324,4 ms	True Positive (TP)
21	Dikenali (Mpok Pepen)	Lolos	Terbuka	75,70%	376,6 ms	True Positive (TP)
22	Teridentifikasi Salah (Mursal)	Lolos	Terbuka	72,17%	344,6 ms	False Positive (FP)
23	Dikenali (Nanda)	Lolos	Terbuka	77,23%	326,4 ms	True Positive (TP)
24	Dikenali (Pak Tio)	Lolos	Terbuka	72,16%	332,3 ms	True Positive (TP)
25	Dikenali (Pak Yadi)	Lolos	Terbuka	78,46%	379,0 ms	True Positive (TP)
26	Dikenali (Rajib)	Lolos	Terbuka	79,78%	346,1 ms	True Positive (TP)
27	Dikenali (Risma)	Lolos	Terbuka	71,54%	338,9 ms	True Positive (TP)
28	Dikenali (Suleha)	Lolos	Terbuka	76,58%	366,4 ms	True Positive (TP)
29	Dikenali (Wak Alex)	Lolos	Terbuka	69,55%	348,2 ms	True Positive (TP)
30	Dikenali (Widia)	Lolos	Terbuka	77,15%	378,7 ms	True Positive (TP)
Rata - Rata				**73,91%**	**351,1 ms**	—

TABEL HASIL PENGUJIAN - SKENARIO: BACKLIGHT

Pengujian	Status Identitas	Status Liveness	Status	Cosine Score	Respon Wajah	Keterangan
1	Dikenali (Fahrul Rosi)	Lolos	Terbuka	66,90%	345,8 ms	True Positive (TP)
2	Dikenali (Vira)	Lolos	Terbuka	70,26%	396,6 ms	True Positive (TP)
3	Dikenali (Aji)	Lolos	Terbuka	68,36%	387,9 ms	True Positive (TP)
4	Dikenali (Andin)	Lolos	Terbuka	67,48%	333,1 ms	True Positive (TP)
5	Tidak Dikenali	Lolos	Terkunci	61,14%	353,2 ms	False Negative (FN)
6	Dikenali (Anjani)	Lolos	Terbuka	76,19%	362,3 ms	True Positive (TP)
7	Dikenali (Aprilia)	Lolos	Terbuka	74,69%	367,2 ms	True Positive (TP)
8	Dikenali (Aulia)	Lolos	Terbuka	76,66%	392,9 ms	True Positive (TP)
9	Dikenali (Ayah Ganis)	Lolos	Terbuka	69,33%	394,8 ms	True Positive (TP)
10	Dikenali (Bang ijal)	Lolos	Terbuka	74,51%	357,7 ms	True Positive (TP)
11	Dikenali (Bu ade)	Lolos	Terbuka	71,33%	356,6 ms	True Positive (TP)
12	Dikenali (Erlan)	Lolos	Terbuka	70,69%	368,7 ms	True Positive (TP)
13	Dikenali (Holijah)	Lolos	Terbuka	70,70%	348,8 ms	True Positive (TP)
14	Dikenali (Joni)	Lolos	Terbuka	67,57%	342,4 ms	True Positive (TP)
15	Dikenali (Julian)	Lolos	Terbuka	69,92%	332,1 ms	True Positive (TP)
16	Teridentifikasi Salah (Kakek Rosi)	Lolos	Terbuka	76,75%	348,6 ms	False Positive (FP)
17	Dikenali (Kenny)	Lolos	Terbuka	73,14%	344,3 ms	True Positive (TP)
18	Dikenali (Martini)	Lolos	Terbuka	71,90%	356,7 ms	True Positive (TP)
19	Dikenali (Miftah)	Lolos	Terbuka	74,21%	334,2 ms	True Positive (TP)
20	Dikenali (Mpok Lia)	Lolos	Terbuka	70,35%	363,1 ms	True Positive (TP)
21	Dikenali (Mpok Pepen)	Lolos	Terbuka	73,66%	349,7 ms	True Positive (TP)
22	Dikenali (Mursal)	Lolos	Terbuka	70,96%	386,4 ms	True Positive (TP)
23	Dikenali (Nanda)	Lolos	Terbuka	74,46%	348,5 ms	True Positive (TP)
24	Dikenali (Pak Tio)	Lolos	Terbuka	70,09%	340,3 ms	True Positive (TP)
25	Tidak Dikenali	Lolos	Terkunci	62,47%	336,5 ms	False Negative (FN)
26	Dikenali (Rajib)	Lolos	Terbuka	75,72%	375,4 ms	True Positive (TP)
27	Dikenali (Risma)	Lolos	Terbuka	68,06%	367,8 ms	True Positive (TP)
28	Dikenali (Suleha)	Lolos	Terbuka	73,12%	399,1 ms	True Positive (TP)
29	Dikenali (Wak Alex)	Lolos	Terbuka	67,90%	370,9 ms	True Positive (TP)
30	Dikenali (Widia)	Lolos	Terbuka	72,75%	355,3 ms	True Positive (TP)
Rata - Rata				**71,04%**	**360,6 ms**	—

Lampiran 7. Link *Source Code*

https://github.com/FahrulRosi/smartdoor-skripsi.git